Berne, le 29 avril 2020

Normes de sécurité pour les appareils connectés à Internet (Internet des objets)

Rapport du Conseil fédéral en réponse aux postulats Glättli 17.4295 du 15 décembre 2017 et Reynard 19.3199 du 21 mars 2019

Table des matières

1 Introduction

Omniprésent dans tous les secteurs de la société, l'Internet des objets (IdO) permet de mettre en réseau des processus industriels au-delà des infrastructures des entreprises. De même, on considère aujourd'hui qu'il est tout à fait normal que les appareils grand public les plus divers soient reliés entre eux et commandés par des capteurs: de l'aide au stationnement dans les voitures aux capteurs de pression dans les brosses à dents, en passant par les micros et les caméras dans les jouets pour enfants.
L'IdO recèle un potentiel énorme dans la mesure où il peut simplifier et rendre plus efficaces de nombreux processus, mais il comporte aussi des risques. Comme pour de nombreuses applications nouvelles, les fabricants qui mettent au point des appareils connectés donnent la priorité à la fonctionnalité et au coût, plutôt qu'aux aspects relatifs à la sécurité. Il n'est dès lors pas surprenant que les médias relatent de plus en plus de problèmes de sécurité liés à des applications IdO et qu'on assiste à une multiplication des cyberattaques exploitant de manière ciblée des faiblesses de l'Internet des objets.
Le présent rapport informe sur la sécurité des appareils connectés afin de montrer comment ces derniers peuvent être mieux protégés contre les cyberattaques. Il explique ainsi les défis et risques propres aux systèmes qui comportent des composants IdO, évoque les cyberattaques les plus connues contre les objets connectés, fait le point sur les directives existantes dans ce domaine, et met en lumière les bases légales qui régissent l'utilisation de l'Internet des objets.

1.1 Contexte

L'IdO a fortement gagné en importance ces dernières années, et les médias comme les politiques sont de plus en plus nombreux à s'y intéresser. L'Internet des objets ajoute aux notions d'accessibilité «en tout temps» (*anytime*) et «partout» (*any place*), que l'on connaît déjà dans le domaine des technologies numériques, celle du «tout connecté» (*anything*). La technologie IdO évolue et se répand à la vitesse de l'éclair, au point que certains estiment que 50 milliards d'objets seront connectés à Internet en 2020. Selon d'autres prévisions, il y aura un jour 200 objets connectés par personne. Dans la mesure où ces objets sont connectés en permanence à Internet, les risques liés à la cybercriminalité augmentent également. Les scénarios vont du détournement de données à l'espionnage, en passant par le sabotage et l'utilisation illégitime des capacités de calcul des appareils. Entre-temps, les médias ont porté de nombreuses cyberattaques à la connaissance du grand public. La population est devenue plus sensible au sujet, notamment après des incidents où des données personnelles ont été divulguées ou utilisées de manière abusive. Le thème de l'IdO mérite une attention particulière dans le contexte industriel: alors qu'une attaque dans une usine risque par exemple de perturber ou d'interrompre la production, les conséquences sont potentiellement bien plus graves pour les exploitants d'infrastructures critiques.

1.2 Mandat

Compte tenu de ces évolutions, il y a lieu d'analyser aussi les conséquences de cette utilisation croissante de l'IdO sur la cybersécurité en Suisse, et de voir ce qu'il faut faire pour garantir au mieux la sécurité des appareils connectés. Conscients de l'importance de cette technologie pour la cybersécurité, le Conseil fédéral et le Parlement ont formulé les mandats d'examen suivants:

- **Postulat 17.4295 Glättli «Normes de sécurité pour les appareils connectés à Internet, qui constituent l'une des principales menaces en matière de cybersécurité»:** le Conseil fédéral est chargé de montrer dans un rapport succinct comment améliorer la sécurité des appareils dans le domaine en croissance exponentielle que représente l'Internet des objets (IdO) et rendre plus difficile leur détournement à des fins criminelles. L'analyse et la présentation porteront notamment sur les points suivants:
  1. bref survol des principales attaques Internet par le biais d'appareils IdO;
  2. état des lieux concernant les directives de sécurité internationales applicables aux appareils IdO (analogues aux dispositions réglant l'admission des appareils électriques) et leur application en Suisse;
  3. introduction de directives internes, valables pour la Confédération et les entreprises qui lui sont proches, assorties de conditions de sécurité quant à l'achat et à la mise en œuvre d'appareils IdO;
  4. introduction de directives de sécurité valables pour les exploitants d'infrastructures critiques: conditions de sécurité à remplir quant à l'achat et à la mise en œuvre d'appareils IdO;
  5. possibilité d'augmenter les chances de voir les lacunes de sécurité IdO reconnues signalées à un service centralisé (Melani, par ex.), au moyen d'obligations d'annoncer ou d'incitations à le faire;
  6. possibilité d'exiger des fabricants qu'ils fournissent des mises à jour de sécurité permettant de pallier les lacunes reconnues, au moins pendant la durée de garantie.

  Le rapport demandé sera clair et concis, et présentera, le cas échéant, des propositions concrètes de mise en œuvre à l'échelon législatif ou réglementaire. À cet égard, l'aide à la création de normes internationales ou la reprise de telles normes prendront autant que possible le pas sur une solution particulariste suisse.
- **Postulat 19.3199 Reynard «Améliorer la sécurité des objets connectés»:** le Conseil fédéral est chargé de présenter un rapport qui aura pour but d'évaluer comment renforcer la sécurité des objets connectés mis sur le marché au regard de la protection des données.
- **Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), champ d'action «Normalisation et réglementation»:** les normes et réglementations dans le domaine des technologies de l'information et de la communication sont des instruments essentiels de protection contre les cyberrisques. Les exigences minimales pour les mesures de protection à adopter renforcent la prévention, et les prescriptions relatives à la gestion des incidents (par ex. obligation de notifier) contribuent à améliorer la réaction. La normalisation et la réglementation sont également importantes dans le contexte international, car elles contribuent à améliorer la transparence de la société du numérique à l'ère de la mondialisation et instaurent un climat de confiance. Dans ce champ d'action, il s'agit de tenir compte des différences considérables entre les secteurs économiques ainsi qu'entre les entreprises de tailles diverses. Le contexte international doit être pris en considération dans tous les cas. Comme le cyberespace ignore les frontières, les normes et les réglementations doivent si possible être compatibles à l'échelle internationale. De même, il convient de vérifier s'il y a lieu d'introduire une obligation de notifier les cyberincidents, et quelles en seraient les modalités.

Le présent rapport fait la synthèse des travaux entrepris à ce jour dans le cadre de ces mandats. Il s'appuie essentiellement sur les résultats d'une étude réalisée sur mandat qui s'intitule «Normes de sécurité dans l'IdO»[1] et qui analyse le poids de l'Internet des objets dans le domaine de la cybersécurité et fournit ainsi des bases pour répondre aux multiples interrogations. Il se sert également de l'analyse des tendances réalisée par le Centre d'études sur la politique de sécurité de

[1] Haute école de Lucerne (HSLU), *Normes de sécurité dans l'IdO – IdO: défis et aperçu des directives informatiques pertinentes*, octobre 2019.

l'EPF de Zurich et publiée sous le titre «The Challenges of Scaling the Internet of Things»[2], qui examine elle aussi l'état d'avancement des recherches à ce sujet au niveau international.

2 Défis pour la sécurité de l'IdO

Nous estimons judicieux, pour notre analyse de la sécurité de l'Internet des objets, de distinguer entre les applications de l'IdO destinées aux clients finaux et celles conçues pour l'industrie. Cela tient surtout au fait que ces deux segments utilisent des stratégies différentes pour garantir la sécurité. Alors que chez les clients finaux, ce sont les appareils en tant que tels qui doivent garantir un certain niveau de sécurité, dans les applications industrielles, il y a aussi lieu de segmenter et de sécuriser les réseaux conformément aux exigences de sécurité. On parle aussi à ce propos de l'Internet industriel des objets (*Industrial Internet of Things*, IIoT).
En comparaison avec les systèmes informatiques (destinés par ex. aux tâches administratives), les systèmes dotés de composants IdO présentent des défis spécifiques en matière de cybersécurité. Le présent chapitre commence par indiquer les risques auxquels il faut veiller en général avec les appareils connectés, dans une optique de sûreté de l'information. Puis il sera question des défis et risques propres aux appareils de l'IdO industriel, dont l'essor dans les infrastructures critiques est un enjeu majeur.

2.1 Exigences générales: manque d'incitations en matière de sécurité de l'IdO

La pression sur les coûts, les délais serrés, ainsi que le manque d'informations et la compréhension limitée de la manière dont les cyberattaquants utilisent les failles de sécurité des appareils connectés engendrent différentes vulnérabilités et l'exploitation de ces dernières. Les utilisateurs d'appareils connectés à Internet ignorent bien souvent qu'ils constituent une cible de choix pour les cyberattaques. Du côté des fabricants, nombreux sont ceux qui ne voient aucun intérêt à proposer des mises à jour logicielles pour leurs appareils ou à équiper ces derniers de fonctions de sécurité spécifiques. Ils raisonnent surtout à court terme et ne songent qu'à vendre un maximum de nouveaux appareils connectés à Internet. Il faut dire aussi que dans l'informatique traditionnelle des systèmes intégrés classiques, la sécurité ne jouait pas un rôle majeur. Et les appareils présentent de nombreuses limitations en matière de capacité des processeurs et d'espace de stockage, de sorte que certains éléments de sécurité peuvent difficilement être installés (absence de chiffrement robuste faute de puissance suffisante au niveau du processeur).
En conséquence, on constate à la fois une absence de demande commercialement intéressante d'appareils connectés sûrs et une offre insuffisante de ces derniers. Les produits grand public en particulier se caractérisent par une forte pression sur les prix, et par un faible niveau de sensibilisation du client final au problème de la sécurité. Et de manière générale, il est peu probable que le marché commence d'exercer une pression suffisamment marquée en faveur d'une amélioration de la sécurité de ces appareils.

2.2 Défis et risques spécifiques liés à l'Internet industriel des objets

Les systèmes de contrôle industriels (SCI), également qualifiés d'IIoT, sont des systèmes informatiques fortement intégrés qui servent au pilotage des processus notamment dans les

[2] Center for Security Studies (CSS) de l'EPF de Zurich, *CYBER DEFENSE PROJECT, Trend Analysis: The Challenges of Scaling the Internet of Things*, August 2019 (en anglais).

infrastructures critiques d'approvisionnement énergétique, de transport ou de traitement de l'eau. Or les cyberattaques lancées contre de tels systèmes de contrôle sont en constante hausse depuis des années.

Des défis ou risques supplémentaires ont fait leur apparition dans ce contexte:

1. Autrefois, les capteurs et les actionneurs[3] d'installations industrielles faisaient partie d'un réseau autonome et n'étaient pas reliés à Internet. Lors de la conception de tels systèmes, la priorité allait à la fiabilité et à la sécurité dans le déroulement des processus. Dans la mesure où ces systèmes n'étaient pas connectés à Internet, ils n'ont pas non plus été protégés spécifiquement contre les cyberattaques. À l'heure actuelle en revanche, soit ces composants de l'Internet industriel des objets (IIoT) sont directement connectés à un réseau de données, soit l'ancien réseau de capteurs-actionneurs est relié à celui de l'entreprise ou à Internet et à des environnements virtuels (informatique en nuage ou *cloud*) via des passerelles (*gateways*)[4]. Si les connexions réseaux ou les espaces de stockage dématérialisés (*cloud*) sont mal sécurisés, une cyberattaque peut exposer les installations industrielles à des situations dangereuses pouvant avoir des répercussions sur l'intégrité physique et la santé humaine.
2. Les fabricants de systèmes de contrôle industriels (SCI) et de systèmes de contrôle et d'acquisition de données en temps réel (appelés plus succinctement «systèmes SCADA», pour *Supervisory Control and Data Acquisition*) proposent de plus en plus de services nécessitant un réseau ouvert et des connexions sans fil. En outre, un nombre sans cesse croissant de capteurs, d'actionneurs et de passerelles sont reliés directement à Internet afin que l'on puisse réagir rapidement et facilement en cas d'erreur dans le système. Jusqu'en 2001, la plupart des attaques subies par les SCI provenaient de l'intérieur, du réseau interne. Ce n'est qu'avec la mise en réseau que des attaques ont pu être menées à partir d'Internet.
3. Les installations industrielles possèdent aujourd'hui des dizaines de microcontrôleurs et de processeurs, comportant des millions de lignes de code de programme – y compris pour la communication des données par Internet. La complexité croissante des applications et la multitude de logiciels sur lesquels elles s'appuient rendent ces installations toujours plus sujettes aux erreurs et vulnérables aux failles de sécurité.

3 Cyberattaques basées sur les appareils connectés à Internet

On distingue quatre types de cyberattaques: ces dernières peuvent cibler les appareils connectés en tant que tels, ce qui se produit lorsque des cybercriminels essaient d'accéder directement à ces appareils afin de les manipuler, de les contrôler ou de les détourner. Les exemples vont d'attaques visant des enceintes connectées (*smart speakers*) ou des écoute-bébé (*babyphones*) pour écouter clandestinement des conversations au déréglage du nombre de tours des moteurs dans les usines de production. D'autres cyberattaques visant des appareils connectés à Internet peuvent servir à pénétrer dans le réseau local par le biais de ces derniers. En l'occurrence, il n'y a plus de manipulation du pilotage des appareils en tant que tels. Dans un troisième scénario, les cyberattaques d'appareils connectés à Internet peuvent viser à créer des réseaux de zombies permettant de cibler d'autres ordinateurs ou serveurs (au moyen d'attaques DDoS[5]). Et dans un quatrième scénario, ce ne sont plus les données mais bien les capacités de calcul des systèmes victimes des attaques qui sont détournées, afin de fabriquer de la cryptomonnaie en exécutant des calculs de minage (*cryptomining* ou *coin mining*).

[3] Actionneur: ensemble d'éléments qui transforment des signaux électriques et du courant en énergie thermique, chimique ou cinétique.
[4] Passerelle: composants (matériels et/ou logiciels) qui établissent une liaison entre deux systèmes.
[5] DoS (*Denial of Service* = déni de service): attaque dont l'objectif avoué est de rendre inaccessibles des systèmes informatiques. On parle d'attaque par déni de service lorsque le déni de service malveillant est causé par un grand nombre de requêtes ciblées, et d'attaque par déni de service distribué (DDoS) lorsque les requêtes émanent d'un grand nombre d'ordinateurs.

Ces possibilités intrinsèques qu'offrent les appareils connectés à Internet en font des cibles de choix des cyberattaques. Les objectifs réels de ces dernières sont abordés en guise d'introduction avant la présentation des principales cyberattaques.

3.1 L'IdO et les divers objectifs des cyberattaques

Appât du gain

La possibilité de gagner illégalement de l'argent explique de très nombreuses cyberattaques. Quiconque parvient à créer un réseau de zombies avec des ordinateurs commandés à distance pourra le louer ou le vendre. Mal sécurisés, les appareils connectés à Internet sont utilisés par les cybercriminels pour créer ces réseaux de zombies[6], qui se servent des capacités de calcul de ces appareils pour mener des attaques DDoS sur des boutiques en ligne, des sites Internet ou d'autres plateformes de services web notamment. Le chiffrement ciblé d'appareils IdO par des rançongiciels (appelés également logiciels de chiffrement ou de chantage, ou *ransomware*) devient lui aussi de plus en plus intéressant pour les crybercriminels. Dans la mesure où le dérèglement de ces appareils peut souvent entraver des fonctions physiques, ceux-ci sont tout à fait adaptés pour faire chanter leurs propriétaires du point de vue des cyberattaquants.

Sabotage

On entend par sabotage le fait de perturber délibérément le déroulement d'un processus. C'est surtout pour les infrastructures critiques que les risques liés au sabotage doivent être pris en considération. Lors d'actes de sabotage, les appareils IdO de ces infrastructures sont attaqués de manière ciblée dans le but de perturber ou de faire cesser la fourniture de biens ou de services de première nécessité comme l'approvisionnement énergétique, les transports ou les moyens de communication, et de générer ainsi de lourds dommages. Cependant, les dégâts potentiels et leurs effets secondaires sur les infrastructures non critiques ne sont pas négligeables non plus. Dans les cas les plus graves, le dérèglement d'un système considéré comme non critique peut ainsi mettre à l'arrêt des installations toutes entières de production de biens industriels importants. Et si ce dysfonctionnement touche simultanément les activités d'une masse critique d'entreprises, les conséquences peuvent être graves pour l'ensemble de l'économie.

Espionnage

L'espionnage consiste à recueillir des informations clandestinement à des fins politiques, économiques ou militaires. Avec la progression rapide du numérique, la recherche de renseignements repose toujours plus sur des programmes informatiques intelligents (maliciels, chevaux de Troie), qui s'installent de manière autonome dans un système afin de capturer et de transmettre des données sensibles. Ces programmes malveillants sont diffusés via les réseaux, ou tirent parti des failles de sécurité pour s'introduire secrètement dans un système. Les appareils connectés à Internet peuvent eux aussi être utilisés à des fins d'espionnage.

3.2 Cyberattaques connues en rapport avec l'IdO

Ces dernières années ont montré à quel point il est facile pour des cyberpirates de prendre le contrôle de milliers, voire de millions d'appareils connectés. Les principales cyberattaques connues en rapport avec des composants IdO sont largement documentées, et les données à leur sujet sont publiquement accessibles. L'étude réalisée sur mandat par la HSLU à propos des «Normes de sécurité dans l'IdO» dresse un aperçu des cyberattaques les plus connues dans lesquelles l'IdO a joué un rôle majeur, et explique succinctement ces dernières.

Parmi les exemples illustres, on peut citer «BASHLITE», «Mirai» et «BrickerBot». La version initiale du logiciel malveillant «BASHLITE» exploitait des failles que présentaient certains appareils, de préférence des routeurs, et connectait les composants compromis au sein d'un réseau zombie. À l'aide de «BASHLITE» et de variations de ce logiciel, des exploitants de réseaux de zombies ont pu compromettre plus d'un million d'appareils en 2016 et utiliser ces derniers pour mener des attaques

[6] Réseau de zombies (*botnet*): ensemble d'une multitude de systèmes «pris en otage» qui peuvent être commandés à distance par l'attaquant.

DDoS. Utilisé pour constituer des réseaux de zombies qui mènent des attaques ciblées contre des appareils connectés à Internet (webcams, routeurs ou enregistreurs vidéo numériques par ex.), le virus «Mirai» a pu infecter des millions d'appareils en quelques semaines. Et en 2016, les répercussions d'une attaque réalisée à l'aide d'une nouvelle variante du réseau de zombies Mirai ont eu un impact majeur sur la disponibilité d'une grande partie d'Internet. Quant au maliciel IdO BrickerBot, il s'est introduit dans divers appareils connectés pour les détruire en écrasant leur système d'exploitation et en supprimant la partition système. On peut encore citer comme exemple une attaque menée en 2015, qui a été annoncée et démontrée, vidéo à l'appui, par les cyberpirates. En l'occurrence, ces derniers ont réussi à prendre le contrôle des systèmes numériques d'un véhicule et à commander ce dernier par Internet. Cette attaque a amené un des plus grands constructeurs automobiles du monde à rappeler 1,4 million de véhicules. Enfin, un autre logiciel puissant, le code malveillant «Triton», a permis à des cybercriminels inconnus, pendant l'été 2017, de prendre le contrôle des systèmes de sécurité protégeant des installations de production dans une usine pétrochimique. Ces criminels auraient pu occasionner des accidents mortels.

3.3 Bilan des cyberattaques

Ces cyberattaques réelles mettent en exergue le potentiel énorme de provoquer, en un laps de temps relativement court, des perturbations voire des destructions au moyen d'appareils connectés à Internet ou par le truchement de ces derniers. De plus, ces attaques montrent clairement que des cybercriminels ont réussi à prendre le contrôle d'appareils connectés ou les ont utilisés comme moyens pour atteindre leurs fins. Complexes et hétérogènes, ces cyberattaques peuvent être dispersées tout comme elles peuvent être ciblées et spécialisées. Pour s'en prémunir globalement, les entreprises devraient utiliser des procédures de sécurité ayant fait leurs preuves, et connaître les appareils connectés fonctionnant dans leur réseau, modifier leurs mots de passe standard, et s'assurer que toutes leurs vulnérabilités ont été corrigées.
Les données disponibles restent toutefois muettes sur les dommages financiers provoqués par les cyberattaques qui ont eu lieu, ce qui s'explique notamment par la grande retenue qu'affichent les entreprises victimes en matière d'annonces et d'informations à ce sujet, par volonté de protéger leurs secrets d'affaires ou par crainte d'une atteinte à leur réputation. Les attaques DDoS aboutissent par exemple souvent à l'indisponibilité momentanée de l'infrastructure informatique. En revanche, les actes de sabotage qui mettent les infrastructures critiques hors service voire les endommagent peuvent avoir de très lourdes conséquences financières[7]. Autrement dit, une bonne stratégie de protection devra prendre en compte non seulement la fréquence ou la portée des cyberattaques, mais aussi le dommage qui pourrait en résulter. Une telle gestion des risques aidera les exploitants de systèmes IdO à définir des mesures adaptées à la situation.

4 Directives internationales sur les appareils connectés à Internet

4.1 Normes et directives internationales sur l'IdO

Il existe peu de normes et de directives internationales officielles sur la sûreté de l'information qui traitent spécifiquement des appareils connectés à Internet, mais il faut s'attendre à ce que ces textes relativement nouveaux évoluent rapidement et que d'autres normes soient édictées. Deux groupes de directives sont distingués ici, selon qu'elles s'adressent aux fabricants d'appareils qui doivent les

[7] En ce qui concerne la Suisse, les résultats de l'enquête sur l'innovation menée en 2016 par le Centre de recherches conjoncturelles de l'EPFZ (KOF) fournit des éléments concrets qui permettent d'estimer le préjudice financier. Cette étude a révélé que les entreprises de plus petite taille étaient plus nombreuses à déclarer une perte de revenu due à une cyberattaque que celles de taille moyenne ou de grande taille, mais que ces dernières devaient toutefois prendre des mesures plus importantes pour réparer les dommages. Voir également «Innovations dans le secteur privé en Suisse», le rapport commandé par le Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI), qui présente les résultats de l'enquête sur l'innovation 2016 réalisée par le Centre de recherches conjoncturelles de l'EPFZ (KOF).

respecter, ou qu'elles définissent le cycle de vie des appareils connectés au sein d'une organisation et visent à en garantir le fonctionnement sûr. Dans le second cas, les directives décrivent les points importants aux différentes phases, du choix d'un appareil jusqu'à son élimination. Il existe naturellement aussi des normes et des directives qui prennent en compte les deux aspects.

4.1.1 Directives destinées aux fabricants

DIN SPEC 27072: IoT-fähige Geräte – Mindestanforderungen zur Informationssicherheit
La norme DIN SPEC 27072, développée par l'Institut allemand de normalisation avec le concours des fabricants, de l'Office fédéral de la sécurité des technologies de l'information (BSI) et d'autres centres de contrôle, a été publiée en mai 2019. Elle fixe les exigences minimales auxquelles doivent satisfaire les objets connectés destinés aux petites entreprises et aux particuliers pour être à l'abri d'attaques élémentaires reposant sur un défaut de conception (par ex. emploi de mots de passe standard). Cette spécification vise à assurer la protection de base de la communication IP des appareils connectés. Elle précise les caractéristiques de sécurité informatiques à prendre en compte lors de la mise au point d'appareils (*security by design*). Ceux-ci seront ainsi à l'abri des cyberattaques de grande envergure lancées à partir d'Internet (comme Mirai).
La nouvelle spécification se limite à formuler des exigences pour des appareils individuels – alors même que les appareils connectés ne sont généralement pas des solutions isolées mais font partie intégrante d'un système informatique. Elle ne tient dès lors pas compte des autres composants d'un tel système (services annexes, applications, logiciels de bureau, etc.).

ETSI TS 103 645: Cyber Security for Consumer Internet of Things
L'Institut européen des normes de télécommunication (ETSI) a publié en février 2019 une norme sur la cybersécurité des appareils grand public connectés à Internet. Sans entrer dans les détails techniques, ce document décrit des procédures éprouvées et généralement reconnues pour garantir la sécurité de ces appareils, avec des dispositions axées sur les résultats. La spécification vise à soutenir toutes les parties impliquées dans le développement et la fabrication des appareils, afin que leurs produits offrent un niveau de sécurité élevé. L'accent y est mis sur les contrôles techniques à effectuer et sur les instructions organisationnelles à suivre pour éviter les principales failles de sécurité.
Le document vise à garantir la sécurité des appareils grand public connectés à Internet, à l'instar des produits suivants:

- jouets pour enfants et écoute-bébé (babyphones),
- produits liés à la sécurité, comme les détecteurs de fumée ou les serrures de porte,
- caméras, enceintes et téléviseurs intelligents,
- dispositifs de suivi de santé portés sur soi,
- systèmes domotiques et d'alarme,
- appareils électroménagers (lave-linge et réfrigérateurs notamment),
- assistants intelligents.

Les entreprises actives dans le développement et la fabrication de tels appareils trouveront dans cette spécification technique les mesures à prendre dans une optique de sécurité.

IEC 62443-3-3: Security for industrial process measurement and control – Network and system security
La Commission électrotechnique internationale (*International Electrotechnical Commmission*, IEC) est l'organisation internationale de normalisation dans le domaine de l'électrotechnique. Elle a publié en 2013 la norme IEC 62443-3-3. Ce document indique comment protéger du point de vue informatique, pendant tout le cycle de vie des installations, leurs systèmes de mesure et de régulation industrielle, avec les réseaux et tous les appareils qui en font partie. On y trouve les exigences en matière de sécurité d'exploitation auxquelles les installations doivent satisfaire, et donc la norme s'adresse en premier lieu à leurs propriétaires et aux exploitants responsables du bon fonctionnement

du système de contrôle industriel (SCI). D'autres groupes s'occupant des SCI sont toutefois aussi concernés par cette spécification et ses exigences pratiques:

- concepteurs de systèmes d'automatisation,
- fabricants d'appareils, de sous-systèmes et de systèmes,
- intégrateurs de sous-systèmes et de systèmes.

Le document prend en compte les points suivants:

- migration/évolution des systèmes existants,
- réalisation des objectifs de sécurité avec les technologies et produits COTS8 existants,
- garanties de fiabilité et de disponibilité des services de communication sécurisés,
- applicabilité aux systèmes, indépendamment de leur taille et de leur niveau de risque (évolutivité),
- conciliation des diverses fonctionnalités (sécurité, cadre juridique, régulation, automatisation) avec les exigences de sécurité actuelles.

4.1.2 Directives relatives à l'exploitation

BSI IT-Grundschutzkompendium: Umsetzungshinweise zum Baustein SYS.4.4 Allgemeines IoT-Gerät

L'Office fédéral allemand de la sécurité des technologies de l'information (BSI) a publié des indications de mise en œuvre pour les appareils connectés à Internet. Elles décrivent la marche à suivre, avec les mesures à prendre au sein de l'organisation pour le bon usage de ces appareils tout au long de leur cycle de vie – de la planification et de la conception jusqu'à la mise hors service – avec les points exigeant une attention spéciale. Ce document vaut pour les appareils connectés en général, quel qu'en soit le champ d'application.

4.2 Directives sur la sûreté de l'information pour les appareils connectés à Internet

À côté des quelques normes et directives internationales à caractère officiel concernant la sûreté de l'information pour les appareils connectés à Internet, on trouve quantité de guides et d'instructions de sécurité visant une utilisation sans danger des appareils et systèmes IdO. Il s'agit de bonnes pratiques en matière de sécurité de l'IdO qui sont publiées par des organisations étatiques ou des alliances, voire par des entreprises. Ces guides axés sur la pratique complètent les normes officielles, dans le but d'améliorer durablement la sûreté de l'information dans les installations de l'Internet des objets. Bien souvent, ces bonnes pratiques renvoient aux directives en vigueur sur la sûreté de l'information en général. Elles portent sur le cycle de vie complet des appareils: mise au point, production, configuration et installation, maintenance et mise hors service.
Quelques exemples d'organisations ayant créé de tels guides figurent ci-dessous:

Cisco: en tant que fabricant de composants et prestataire dans le domaine des réseaux de données, Cisco a publié l'ouvrage «Orchestrating and Automating Security for the Internet of Things: Delivering Advanced Security Capabilities from Edge to Cloud for IoT».

DHS: l'Agence de la cybersécurité et de la sécurité des infrastructures du Ministère américain de la sécurité intérieure (CISA-DHS) a élaboré le document «Strategic principles for securing the Internet of Things».

ENISA: l'Agence de l'Union européenne chargée de la sécurité des réseaux et de l'information (ENISA) est à l'origine de nombreuses publications sur la sûreté de l'information. Certaines se réfèrent expressément à des thèmes de l'IdO (villes intelligentes, transports publics, hôpitaux, maison intelligente, fabrication, aéroports, etc.).

[8] L'abréviation COTS, qui correspond à «commercial off-the-shelf», ou à «components-off-the-shelf», renvoie à des produits fabriqués en série dans le secteur de l'électronique ou des logiciels (logiciels standards), en tous points similaires, qui sont conçus et vendus en grandes quantités (et prêts à être utilisés).

GSMA: la GSMA, qui représente les intérêts des opérateurs de téléphonie mobile du monde entier, a publié des consignes de sécurité sur l'IdO.

IoTSF: l'organisation à but non lucratif *IoT Security Foundation (IoTSF)* est à l'origine d'une série de publications consacrées à la sûreté de l'information et à l'IdO, intitulées «IoT Security Foundation Best Practice Guidelines».

NIST: Institut national américain des normes et de la technologie (NIST).

4.3 Directives générales en matière de sûreté de l'information

Les normes et directives en matière de sûreté de l'information, soit notamment la suite ISO/CEI 27000, le cadre de cybersécurité du NIST (*Cybersecurity Framework*) ou les directives du BSI (*IT-Grundschutz-Kompendium*), décrivent les moyens d'atteindre au sein des organisations la sûreté de l'information nécessaire. On y voit notamment comment mettre en place un système de gestion de la sécurité de l'information (*information security management system*, ISMS). Ces normes à caractère général sont bien entendu aussi valables pour les systèmes comportant des appareils connectés à Internet. Cependant, il y a lieu de tenir compte spécifiquement des risques et défis particuliers qui caractérisent les appareils connectés à Internet lors de l'adaptation et de la mise en œuvre de ces directives.

4.4 Directives sur les appareils connectés à Internet: résumé

Peu de normes et de directives internationales officielles relatives à la sûreté de l'information portent spécifiquement sur les appareils connectés. Et les études sur la sûreté de l'information ainsi que sur l'IdO mettent en exergue une problématique: il existe des normes très diverses et de nombreux guides dans différents domaines thématiques, mais aucune norme n'a pu s'imposer à ce jour, et les fabricants ne savent pas à quelles normes ils doivent se référer. Il serait par conséquent souhaitable de promouvoir l'harmonisation des initiatives et prescriptions visant à la sécurité de l'IdO. L'«*Alliance for the Internet of Things Innovation, AIOTI*» a récemment publié deux rapports sur ce sujet, dans lesquels elle présente les normes et les solutions à source ouverte qui peuvent être appliquées pour élaborer des prescriptions dans le domaine des objets connectés, ainsi que les lacunes auxquelles il y a lieu de remédier en priorité dans le cadre de la normalisation.
Outre les différentes approches en la matière, il existe quantité de guides et de bonnes pratiques consacrés à la sûreté de l'information. Ces documents renvoient en général à des normes communes ayant fait leurs preuves dans le domaine de la sécurité informatique. Tant que les particularités indiquées de l'IdO sont prises en compte, ces normes éprouvées à maintes reprises conviennent aussi aux systèmes informatiques incluant des appareils connectés. Des directives concernant spécialement les appareils reliés à Internet compléteront ces directives générales sur la sûreté de l'information, par exemple pour l'IdO dans le segment grand public, pour les applications industrielles (IIoT) ou pour les infrastructures critiques.
Il ne suffit toutefois pas d'élaborer des normes et des bonnes pratiques pour renforcer la sécurité des applications IdO. L'aspect essentiel est leur mise en œuvre dans la pratique. Cependant, ce sont les entreprises et les organisations concernées qui doivent répondre de leur propre protection. Chaque entreprise est en effet responsable de la sécurité de son infrastructure informatique. Autre initiative qui pourrait aussi fournir des résultats intéressants à ce sujet pour la Suisse, le projet européen SerIoT[9] (*Secure and Safe Internet of Things*) a pour objectif de créer une plateforme IdO qui met l'accent sur la cybersécurité et le respect de la vie privée par les systèmes connectés à Internet.

[9] https://seriot-project.eu/

5 Mise en œuvre des normes au niveau de la Confédération et des infrastructures critiques

Les directives de sécurité applicables à l'administration fédérale et aux entreprises proches de la Confédération ou aux exploitants d'infrastructures critiques ne prévoient pas de règles divergentes pour la cybersécurité des appareils connectés à Internet. Les normes, les bonnes pratiques et les processus visant à atteindre une sécurité suffisante contre les cyberattaques y sont identiques. En fonction des exigences des organisations, divers niveaux de sécurité peuvent être définis pour une norme donnée compte tenu des risques. L'Office fédéral pour l'approvisionnement économique du pays (OFAE) a édicté pour les entreprises, et en particulier pour les exploitants d'infrastructures critiques, une «norme minimale pour améliorer la résilience informatique», qui n'est pas directement contraignante sur le plan juridique. Cette norme minimale se fonde sur le cadre de cybersécurité du NIST et inclut des ajouts ponctuels provenant d'autres normes industrielles reconnues au niveau international (ISO 2700x, COBIT, ENISA «NCSS Good Practice Guide» et BSI 100-2). L'objectif de la «norme» recommandée est de fournir aux entreprises et aux organisations un outil qui leur permet d'améliorer sur une base individuelle la résilience de leur infrastructure informatique.

6 Aspects juridiques de l'IdO

À l'instar d'autres technologies, le recours à l'IdO doit lui aussi impérativement prendre en considération le contexte juridique applicable. Les interrogations relatives à l'utilisation des données ainsi qu'à la garantie légale et à la garantie commerciale des appareils connectés à Internet sont présentées brièvement ci-dessous. L'obligation d'annoncer les cyberincidents est également abordée dans ce contexte.

6.1 Protection des données

La collecte et l'évaluation des données comptent parmi les principales raisons pour lesquelles l'IdO est utilisé. Or les appareils échangent, par les réseaux et Internet, des informations qui permettent d'établir un lien avec une personne physique dans certaines circonstances. Un tel lien n'a pas besoin d'être immédiat (données spécifiques), il suffit qu'il puisse être établi au prix d'un effort raisonnable (données identifiables). Dès que c'est le cas (compteurs intelligents, informations sur des produits de la région, etc.), il faut se conformer à la législation sur la protection des données. Au niveau des opérateurs privés (entreprises par exemple), le traitement des données personnelles n'est en principe soumis à aucune base légale spécifique. Ce n'est que lorsque cette activité porte atteinte à la personnalité dans un cas concret que l'entreprise doit fournir un motif justificatif (art. 12 LPD; art. 26 P-LPD[10]). Ce motif justificatif peut être un texte de loi, le consentement de la personne concernée ou un intérêt privé ou public prépondérant au traitement des données (art. 13 LPD; art. 27 P-LPD). Pour les organes fédéraux en revanche, c'est le principe de légalité qui prévaut, car ces derniers ne sont en droit de traiter des données personnelles que s'il existe une base légale. En dérogation à cette règle, le traitement de ces données peut, dans un cas d'espèce, s'appuyer entre autres sur le consentement de la personne concernée (art. 17 et 19 LPD; art. 30 et 32 P-LPD). Il faut se souvenir ici que toute opération relative à des données personnelles est assimilée au traitement de données, et que le système de gestion des données doit respecter toutes les exigences de protection de ces dernières. Si la législation sur la protection des données régit le traitement des données, elle n'énonce pas les exigences à respecter lors de la mise sur le marché des produits. Les exigences minimales en matière de sécurité des données sont précisées dans l'ordonnance relative à la loi fédérale sur la protection des données (OLPD; art. 7, al. 2, LPD; art. 7, al. 3, P-LPD), dont les dispositions seront examinées

[10] Projet de loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales (P-LPD) FF **2017** 6803.

après la révision complète de la LPD. Le projet de révision de la LPD (P-LPD) ancre en outre expressément dans la loi le principe de la protection des données par des mesures techniques. En application de l'art. 6, al. 1, P-LPD, le responsable du traitement des données est tenu de mettre en place, dès la conception du traitement, des mesures techniques et organisationnelles afin de respecter les prescriptions de protection des données. Par ailleurs, le Préposé fédéral à la protection des données et à la transparence (PFPDT) devrait obtenir des compétences décisionnelles. En cas de traitement illicite de données notamment, ce projet prévoit que le PFPDT pourra interdire ce traitement, et ordonner la destruction des données personnelles concernées. Il pourrait aussi exiger que des mesures techniques et organisationnelles appropriées soient prises pour garantir la sécurité (voir l'art. 45, al. 1 et 3, en relation avec l'art. 7 P-LPD). De plus, l'art. 55, let. c, P-LPD énonce désormais des dispositions pénales en cas de violation intentionnelle des exigences minimales de sécurité des données.
Certaines informations sans référence à des individus que transmettent les appareils connectés permettent également d'identifier d'éventuels secrets d'affaires ou de fabrication. En l'occurrence, il est essentiel que les parties concernées s'informent mutuellement et s'accordent sur la finalité de la collecte des informations (maintenance par ex.) et sur la date à laquelle ces dernières seront effacées. Faute d'un tel accord, une dénonciation pour espionnage économique ou pour infraction au droit de la concurrence est à craindre. Les cadres dirigeants qui transmettent ou reçoivent de telles informations doivent désormais envisager ces thèmes, en vertu de leur devoir de diligence, comme faisant partie de leur champ d'activité professionnelle et réduire les risques qui en découlent. S'ils ne le font pas, ils s'exposent à être tenus personnellement responsables en cas d'incident. Si de telles informations sont traitées légitimement, il se peut très bien que les résultats soient soumis au droit d'auteur, et donc qu'ils ne soient que partiellement exploitables. Dans le cas d'organisations étatiques, les résultats du traitement de données peuvent être soumis au principe de publicité ou à des exigences de transparence (ouverture des données).
Le traitement illégal des données peut contrevenir tant au droit privé qu'au droit public, et engager la responsabilité civile ou aboutir à des sanctions pénales. Ce sont en effet des lois en vigueur qui sont bafouées, même si les faits se produisent dans le monde virtuel et non dans le monde réel. Il est indispensable de disposer de connaissances en informatique légale et d'outils spécifiques adéquats pour pouvoir prouver l'existence des infractions en question. Souvent, les coûts de l'obtention des preuves sont nettement plus élevés dans l'univers virtuel, notamment parce que les traces disponibles comme les adresses IP ne permettent pas nécessairement de remonter aux personnes responsables.

6.2 Garantie en raison des défauts de la chose (garantie légale), garantie commerciale et sécurité des produits

Le vendeur répond des défauts de la chose achetée en application des dispositions du code des obligations sur la garantie en raison des défauts de la chose vendue (art. 197 ss CO). Il y a défaut lorsqu'un élément enlève à la chose vendue soit sa valeur, soit son utilité prévue, ou les diminue dans une notable mesure, ainsi qu'en cas d'absence d'une qualité promise par le vendeur (art. 197, al. 1, CO). Les qualités de la chose en tant que telle, qui sont promises pour un temps déterminé sont appelées garanties non autonomes et considérées comme des promesses au sens de la garantie en raison des défauts de la chose vendue[11]. Ces garanties s'opposent à une clause de porte-fort autonome (art. 111 CO), par laquelle le vendeur promet un résultat futur qui dépasse la nature de la chose vendue selon le contrat parce que ce résultat dépend essentiellement d'autres facteurs futurs qui sont sans lien avec les qualités matérielles de la chose et sur lesquels le vendeur n'a aucune emprise[12]. La garantie commerciale constitue une promesse de prestation de nature abstraite; il s'agit d'un engagement volontaire du vendeur, que la loi ne règle pas de manière plus détaillée.
Il est difficile d'établir si des lacunes de sécurité du logiciel d'un objet connecté constituent un défaut matériel, ni dans quelles conditions le cas échéant. Dans un premier temps, il importe surtout de

[11] TF 4A_220/2013 (consid. 4.3.1)
[12] ATF 122 III 426 (consid. 4 et 5c); TF 4A_220/2013 (consid. 4.3.1)

déterminer si le vendeur s'est engagé expressément ou tacitement dans le contrat de vente à mettre le logiciel à disposition. Tel devrait en général être le cas lors de l'achat d'appareils avec logiciel intégré. Cependant, s'il ne s'est pas engagé à cet égard, on ne peut pas considérer qu'une lacune de sécurité constitue toujours un défaut matériel. En pareil cas, l'acheteur peut uniquement s'adresser au fabricant du logiciel. Toutefois, même lorsque le vendeur s'est engagé dans le contrat de vente à mettre le logiciel à disposition, la question de savoir si des lacunes de sécurité pourront un jour être qualifiées de défauts matériels n'a pas été tranchée. Les lacunes de sécurité ne constituent pas en tant que telles une restriction de l'usage. Sont en outre considérés comme des défauts matériels uniquement les défauts qui étaient déjà présents au moment du transfert du risque. L'autre question qui se pose donc surtout est de savoir ce qu'il en est des lacunes de sécurité qui apparaissent ultérieurement. À notre connaissance, il n'y a encore aucune jurisprudence à ce sujet pour l'instant. Si l'acheteur constate un défaut, il doit contester ce dernier sans délai auprès du vendeur. L'acheteur a alors le choix soit de faire résilier la vente soit de réclamer une réduction du prix d'achat. Pour les choses fongibles, il peut aussi demander le remplacement de la chose livrée. Pour les autres préjudices (en cas de perte de production notamment), il peut exiger du vendeur qu'il l'indemnise du dommage, à moins que ce dernier ne prouve qu'il n'a commis aucune faute. Les droits liés à la garantie en raison des défauts peuvent par ailleurs être restreints ou modifiés contractuellement, dans les CGV par exemple. Les prétentions au titre de la garantie en raison des défauts se prescrivent par deux ans après la livraison de la chose vendue. Le vendeur qui livre des choses nouvelles à des consommateurs ne peut pas raccourcir ce délai; mais il peut le raccourcir d'un an s'il s'agit de choses d'occasion. Ces délais courts peuvent poser un problème pour les produits dont on attend habituellement une durée de vie plus longue, car dans certaines circonstances, l'incitation à remédier aux lacunes de sécurité après le délai de prescription est faible pour le vendeur ou le fabricant. Compte tenu de cette situation juridique floue, les acheteurs seraient bien avisés d'exiger du vendeur qu'il leur fournisse des promesses ou des garanties (autonomes) réglant globalement et clairement la question des mises à jour logicielles et les lacunes de sécurité. Dans l'industrie ou en domotique, les durées de vie des appareils connectés à Internet peuvent souvent avoisiner ou dépasser dix ans. Une convention contractuelle prévoyant une période de maintenance suffisamment longue pour les logiciels est fortement recommandée dans ces cas de figure. Si le raccordement à d'autres systèmes constitue un élément important, la publication des interfaces possibles doit en outre être garantie contractuellement pendant toute la durée d'exploitation attendue de l'appareil. Cette obligation de mise à disposition permanente de toutes les fonctionnalités peut être conçue sous forme de contrat de maintenance autonome (avec des éléments du droit des contrats: vente, bail, contrat d'entreprise et mandat), ou en tant qu'obligation contractuelle accessoire[13]. Si une disposition expresse faisait défaut, il y aurait lieu de vérifier au cas par cas si cette obligation n'a pas été convenue tacitement – sous forme de contrat autonome ou d'obligation accessoire autonome en vertu du contrat de vente. Lors de l'achat d'un appareil connecté incluant un logiciel, on peut en général partir du principe que l'obligation de mettre le système à disposition et d'en assurer la maintenance fait partie intégrante du contrat de vente si ce dernier ne l'exclut pas explicitement. On peut en effet supposer une certaine durée de vie de l'appareil dans le cadre de son utilité prévue. La doctrine soutient qu'en ce qui concerne la durée de cette obligation de mettre le système à disposition et d'en assurer la maintenance, l'aspect déterminant est la durée de vie qui peut être attendue en général des appareils du même type[14]. Il est possible qu'on puisse faire valoir la violation de cette obligation contractuelle de manière autonome, à savoir indépendamment des règles de la garantie en raison des défauts de la chose, ou uniquement en appliquant ces dernières par analogie et avec un délai de prescription d'autant plus long. Cependant, il n'y a pas non plus à notre connaissance de jurisprudence ou d'avis clair et majoritaire dans la littérature au sujet de cette question.

[13] Voir M. Eggen, Gewährleistung bei vernetzten Geräten, RSDA 2019, 358, 364 s, ainsi que les ouvrages qui y sont cités (en allemand)
[14] Voir M. Eggen, Home Smart Home – Eine privatrechtliche Einordnung von Lösungen für intelligentes Wohnen, PJA 2016, 1131 ss, 1139 (en allemand)

6.3 Obligation d'annoncer

Dans le contexte de la protection des données, la révision complète de la LPD comporte une obligation d'annoncer toute violation de la sécurité des données. Et si une telle violation entraîne vraisemblablement un risque élevé pour la personnalité ou les droits fondamentaux des personnes concernées, le responsable du traitement l'annonce dans les meilleurs délais au PFPDT (art. 22, al. 1, P-LPD). Dans certaines circonstances, le responsable du traitement informe par ailleurs les personnes concernées afin de leur permettre de prendre elles-mêmes des mesures pour protéger leurs données (art. 22, al. 4, P-LPD).
Pour les cyberincidents, la Suisse ne connaît cependant ni obligation générale d'annoncer ni devoir de notifier les vulnérabilités. L'échange d'informations sur les cyberincidents ou sur les failles de sécurité connues au niveau des infrastructures critiques d'approvisionnement énergétique, des télécommunications, du secteur financier ou des assurances a lieu sur une base volontaire par l'intermédiaire de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Compte tenu de l'évolution des cyberrisques, la question qui se pose naturellement, face à l'usage de plus en plus intensif d'un nombre croissant d'appareils connectés, est aussi de savoir si cet échange d'informations sur une base volontaire suffit pour identifier les menaces à un stade précoce dans tous les secteurs.
Cette question doit toutefois être examinée de manière générale et pas spécifiquement par rapport à l'IdO. Dans le cadre de la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), la Confédération réfléchit, de concert avec les autorités compétentes et les milieux économiques, à des variantes d'une obligation d'annoncer les incidents graves concernant la sécurité des infrastructures critiques. Le Conseil fédéral se fondera sur les résultats de cette réflexion pour prendre, d'ici fin 2020, des décisions de principe sur l'introduction d'obligations d'annoncer.

6.4 Perspectives: évolution du cadre juridique dans l'UE

De nombreux États réfléchissent actuellement aux adaptations possibles ou nécessaires de la législation pour renforcer la sécurité de l'IdO. Les travaux entrepris par l'UE à cet égard sont particulièrement intéressants pour la Suisse. Les évolutions pertinentes actuelles du cadre juridique européen sont présentées ci-dessous. Cette liste ne prétend nullement être exhaustive, et il n'est pas non plus possible de prévoir à présent les démarches que l'UE entreprendra. Le Conseil fédéral suivra les évolutions futures en analysant en permanence les conséquences éventuelles de ces dernières pour la Suisse.
En ce qui concerne les questions susmentionnées à propos de la garantie en raison des défauts de la chose, de la garantie commerciale et de la sécurité des produits, la révision de la directive européenne sur les contrats de vente de biens (directive 2019/771 du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens) est un texte majeur. Cette directive prévoit, pour l'achat de biens comportant des éléments numériques, que le vendeur est tenu de veiller à ce que le consommateur reçoive les mises à jour de sécurité qui sont nécessaires au maintien de la conformité de ces biens. Lorsque le contrat de vente prévoit une opération de fourniture unique du contenu numérique ou du service numérique, cette obligation vaut pour la période à laquelle le consommateur peut raisonnablement s'attendre, eu égard au type et à la finalité des biens et des éléments numériques et compte tenu des circonstances et de la nature du contrat. Cependant, la durée de la garantie légale est généralement de deux ans lorsque le contrat de vente ne prévoit pas la fourniture continue des contenus numériques[15]. Les États membres de l'UE doivent mettre en œuvre ces nouvelles règles d'ici au 1er janvier 2022.
Une autre évolution intéressante se dessine dans le domaine de l'Internet des équipements radio, à savoir les objets connectés entre eux par des ondes radioélectriques. En se fondant sur la législation

[15] Voir Y. Atamer/S. Hermidas, Die neue EU-Richtlinie zum Verbrauchsgüterkauf, PJA 2020, 48, 56 s. (en allemand)

en vigueur (directive sur les équipements radioélectriques; 2014/53/UE)[16], la Commission européenne a la possibilité d'imposer des exigences supplémentaires par un simple acte délégué. Elle a d'ailleurs lancé une consultation publique à cette fin en 2019. Les résultats de cette consultation sont attendus prochainement, et les préparatifs en vue d'un acte délégué avancent rapidement. Dans la mesure où la Suisse a repris la directive sur les équipements radioélectriques dans sa législation, ces évolutions présentent un intérêt tout particulier. En reprenant également l'acte délégué, notre pays pourrait renforcer les exigences de cybersécurité imposées aux objets connectés à Internet sans fil. La Confédération participe aux travaux de l'UE dans le cadre du groupe d'experts en charge de la directive sur les équipements radioélectriques par l'intermédiaire de l'Office fédéral de la communication (OFCOM).

7 Conclusion

Compte tenu du fait que le nombre d'appareils raccordés à Internet va encore augmenter, tout laisse présager également une intensification des cyberattaques basées sur l'IdO. Les attaques décrites montrent le risque inhérent à de tels incidents. Il existe plusieurs approches pour garantir la sécurité de l'Internet des objets. Un constat important est qu'en raison des nombreuses utilisations possibles de l'IdO, les utilisateurs d'appareils connectés peuvent eux-mêmes compromettre fortement la sécurité de ces derniers, soit en prenant trop à la légère les principes visant un usage sûr de ces appareils, soit en utilisant des produits non sécurisés de fabricants inconnus. En l'occurrence, il y a lieu de continuer à sensibiliser la population et de l'inciter à respecter les règles fondamentales de comportement afin que ces appareils soient employés en toute sécurité.
Quant aux entreprises qui exploitent des systèmes connectés, il est essentiel qu'elles considèrent que l'IdO fait partie intégrante de leur infrastructure informatique, et qu'elles mettent aussi en œuvre des procédés dûment éprouvés pour garantir leur sécurité. En outre, le fait de prendre en considération le préjudice potentiellement engendré par ces cyberattaques permet de définir la stratégie de défense appropriée contre ces dernières. Une telle gestion des risques aidera les exploitants de systèmes IdO à définir des mesures adaptées à la situation. Les normes et directives actuelles en matière de sécurité informatique fournissent déjà une bonne base à cet égard. Des guides et la promotion d'échanges d'informations entre utilisateurs peuvent contribuer à élargir leur application à l'IdO. Parallèlement, les fabricants doivent prendre leurs responsabilités et satisfaire par exemple à des exigences minimales en matière de sécurité de l'information et de protection des données lors de la mise en service de leurs produits. Même si de nombreux fabricants n'assument pas ou pas suffisamment cette responsabilité, différents concepteurs voient aussi de plus en plus la sécurité comme une possibilité de se distinguer des fabricants de produits à prix cassés en appliquant des normes de qualité plus strictes, pour ainsi s'imposer sur ces marchés concurrentiels. Les États peuvent soutenir cette évolution en rédigeant des directives, des guides ou des prescriptions. Mais il faut dire en l'occurrence que différentes bases normatives et normes internationales bien établies destinées aux fabricants s'appliquent aussi à l'IdO. En mettant systématiquement en œuvre les directives existantes, les fabricants et exploitants d'appareils et de systèmes IdO peuvent déjà atteindre un niveau élevé de cybersécurité. Il en va de même sur le plan juridique. Ainsi, les dispositions de la législation sur la protection des données s'appliquent par exemple aussi au domaine de l'IdO, et les bases légales actuelles concernant la garantie légale et la garantie commerciale offrent des possibilités de placer les fabricants face à leurs obligations. Si d'autres dispositions légales ou directives doivent être rédigées spécifiquement pour l'IdO, il faut que ce soit dans le cadre d'une coopération étroite au niveau international. En effet, les prescriptions édictées isolément par certains États ont un effet trop limité sur les fabricants et feraient naître des distorsions non souhaitables sur le marché.

[16] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32014L0053&from=EN

Le Centre national pour la cybersécurité prendra en considération et suivra de près les points-clés évoqués dans le présent rapport au sujet des normes de sécurité des appareils connectés à Internet lors de la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Il faudra voir au niveau sectoriel dans quelle mesure les solutions proposées dans le champ d'action «Normalisation et réglementation» en particulier sont supportables économiquement. Ces travaux seront menés de concert avec tous les départements concernés, avec les cantons, et avec les milieux économiques.