



L'INTERNET DES OBJETS (IDO) POUR UNE CULTURE DE TRAVAIL HYBRIDE

ENG221



le **cnam**
Ecole d'ingénieurs **eicnam**



2021-2022
VOLLE CYRIL
CNAM Aix-en-Provence



1 TABLE DES MATIÈRES

1	Table des matières.....	1
2	Introduction.....	2
3	Internet des objets.....	2
3.1	Définition de l'Internet des Objets.....	2
3.2	Histoire de l'internet des objets.....	3
3.3	Évolutions et développements.....	3
3.4	Les objets en entreprise.....	5
3.5	Technologie utilisés et standardisation.....	7
3.6	Sécurité et protection de la vie privée.....	11
4	Travail hybride.....	14
4.1	Définition du travail hybride.....	14
4.2	Histoire et évolutions.....	14
4.3	La tendance « Flex Office ».....	16
4.4	Pandémie de Covid 2019.....	16
4.5	Sécurisation et risques.....	17
4.6	Les chiffres en France.....	19
4.7	Conséquences psychologiques et culture d'entreprise.....	21
5	L'émergence du « Smart Office ».....	22
6	Impact écologique et effet rebond.....	24
7	Conclusion.....	26
8	Bibliographie.....	27
9	Illustrations.....	30

2 INTRODUCTION

Nous vivons dans un monde de plus en plus connecté, des outils se développent pour nous faciliter la vie, échanger et travailler de façon nomade.

Ce sujet va aborder l'application de l'internet des objets dans un contexte de travail hybride.

La pandémie a, par exemple, poussé les entreprises à utiliser ce mode de travail. Seulement, sans préparation, les premiers problèmes n'ont pas tardé avec des attaques multiples dues souvent à des mises en place précipitées.

L'internet des objets, pour sa part, se retrouvent tout autour de nous, il peut nous apporter des solutions pour améliorer l'entreprise mais il ne faut cependant pas négliger aussi les risques qu'ils peuvent provoquer en matière de sécurité et confidentialité.

Comment vont évoluer ces solutions au sein de nos modes de travail et comment anticiper les risques et mettre en place de façon pérenne ces outils ? Nous allons essayer de répondre à ces questions au travers de la présentation de ces technologies, qui changent l'organisation des entreprises, mais aussi l'impact de celles-ci dans les villes et dans notre quotidien, elles peuvent alors devenir autant des atouts que des contraintes selon comment elles sont utilisées.

3 INTERNET DES OBJETS

3.1 DÉFINITION DE L'INTERNET DES OBJETS

L'internet des objets (en anglais IoT Internet of Things) regroupe tous les objets connectés à internet, on retrouve de plus en plus des objets connectés chez soi avec des enceintes, de la domotique, la télévision mais aussi en dehors avec les véhicules connectés, les caméras ...

La définition officielle est : « infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution » (télécommunications, 2012)

3.2 HISTOIRE DE L'INTERNET DES OBJETS

Son origine est liée au début de la mise en place de l'internet tel qu'on le connaît avec le premier protocole IP (en 1981 avec le TCP/IP), on estime que premier produit de l'internet des objets est né dans les années 80 avec une machine à soda connectée, celle-ci permettait d'avoir accès, via internet, au statut de la machine, à son stock ainsi que la température du soda, elle avait été développée par le département informatique de (Université Carnegie Mellon (Pittsburgh, 1982).



Figure 1 Machine à soda connectée

3.3 ÉVOLUTIONS ET DÉVELOPPEMENTS

Avec le développement du numérique l'internet des objets s'est développé en premier au niveau des entreprises et administrations avec le

développement de capteur de toutes sortes (température, humidité, présence ...) qui se sont interconnectés afin d'avoir une gestion en temps réel mais c'est surtout avec l'avènement des technologies mobiles et la mise en place de solutions associées que l'essor a été le plus important (Quelle gouvernance pour l'IoT ?), on estime que d'ici 2025 c'est plus de 150 milliards d'objets qui vont se connecter entre eux (Society : Build digital democracy , 2015)

On retrouve, de nos jours, l'internet des objets dans tous les domaines (réfrigérateur, voiture, enceinte, caméra, domotique ...).

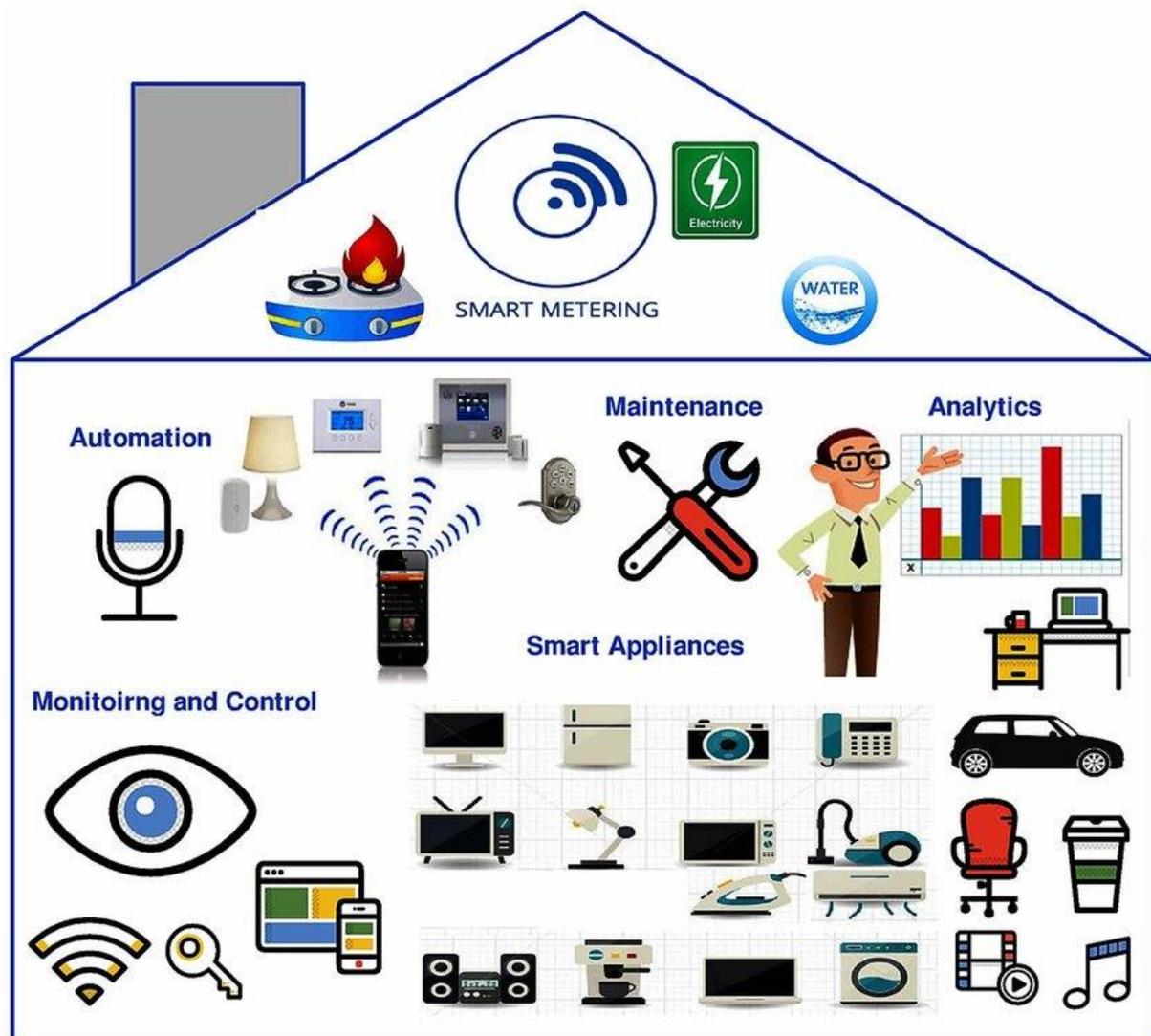


Figure 2 Exemples de l'internet des objets

Dans le futur on prévoit qu'avec l'intelligence artificielle ces objets pourraient fonctionner de manière autonome et pouvoir ainsi s'adapter aux usages et à l'environnement.

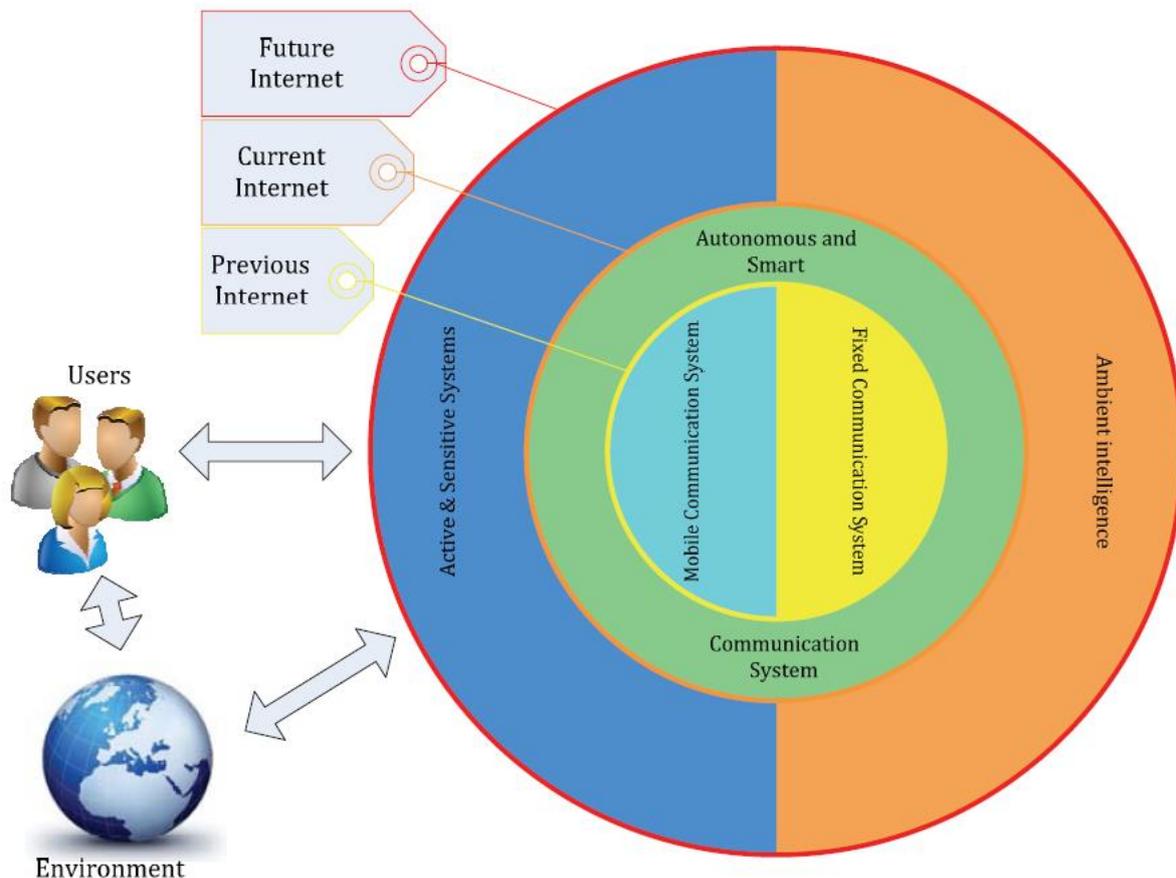


Figure 3 Le livre blanc : Objets communicants et Internet des objets (Carnot, 2011)

3.4 LES OBJETS EN ENTREPRISE

L'internet des objets s'est développé en entreprise pour le suivi des employés (badgeage, congés ...) et aussi pour l'accès aux services (réservation de salle, ouverture de véhicules...).

Il est aussi utilisé dans de nombreux domaines pour faciliter et améliorer les processus : calcul du poids de déchets, géolocalisation des véhicules, sécurisation des accès, suivi des productions ...

Dans les grandes entreprises de puissants systèmes se développent alliant internet des objets, big data et digitalisation afin de monitorer, prédire et gérer l'ensemble des process.

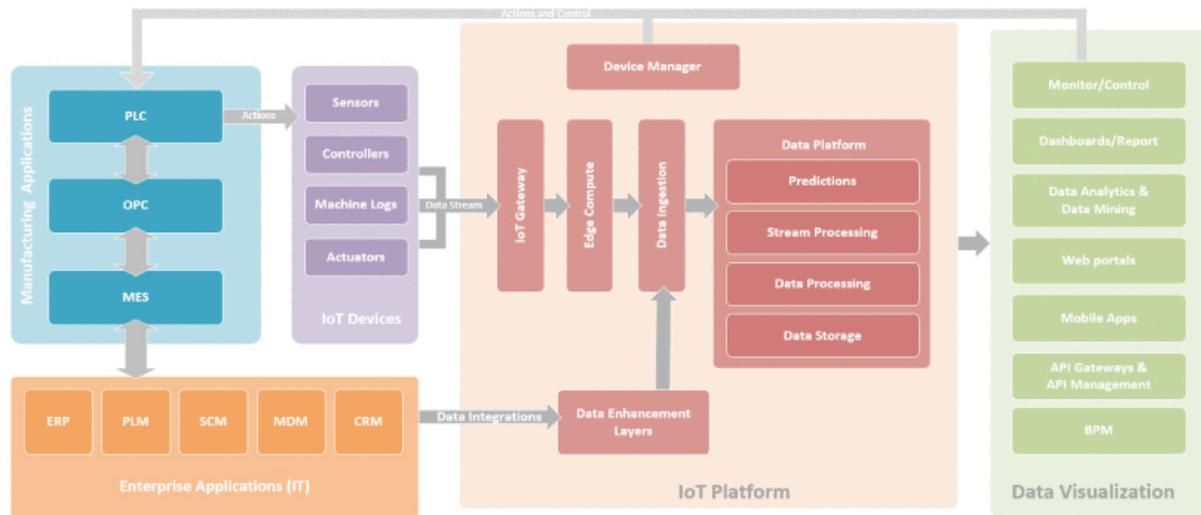


Figure 4 Exemple de schéma dans une usine (Illa, 2018)

Pour traiter les données au plus près des process on utilise l'Edge Analytics, cette technologie est venue du constat de la quantité massive de données générée par ces capteurs et qui a amené, afin de ne pas encombrer le système d'information et de sécuriser les infrastructures, à traiter une partie des calculs directement au sein des objets et avec des réseaux spécifiques.

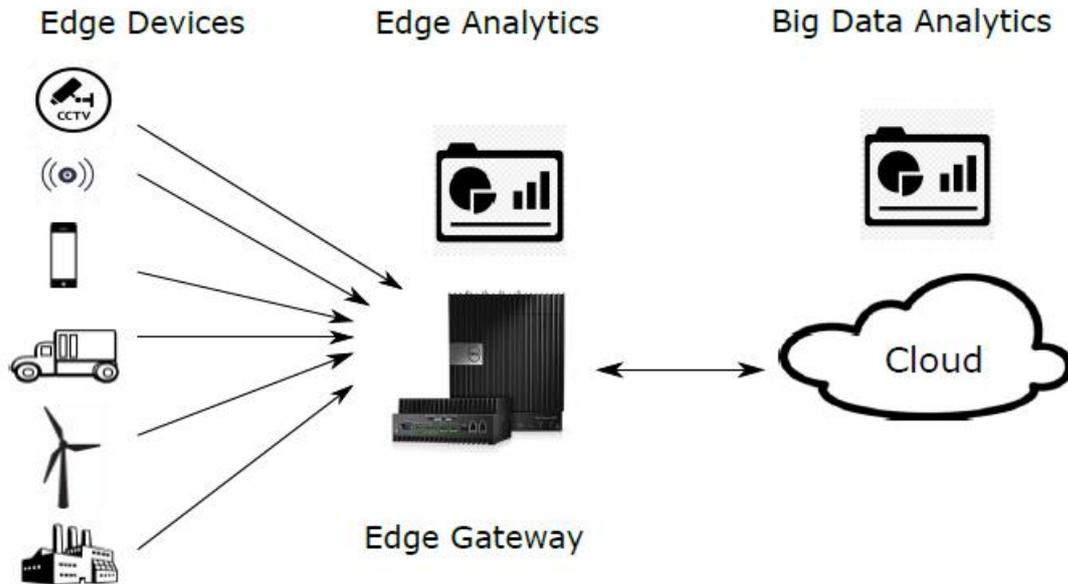


Figure 5 Edge analytics et Big data (Nayak, 2021)

3.5 TECHNOLOGIE UTILISÉS ET STANDARDISATION

Les technologies que l'on retrouve dans l'internet de l'objet pour la connectivité sont les plus classiques : wifi, Ethernet, 4G, Bluetooth, NFC... Mais aussi des protocoles propres à ces solutions tel que Zygbee, dont les premiers appareils voient le jour en 2005, et qui a bénéficié d'une large diffusion du fait de sa faible consommation (une pile pouvant alimenter un appareil pendant des années), de son fonctionnement en maillage permettant une couverture étendue ainsi que par sa facilité d'utilisation et d'intégration (20% de code permet de gérer la connectivité comparé aux solutions de l'époque), il a depuis été rattrapé, à partir de 2010, par le Bluetooth Low Energy qui a des avantages similaires avec un débit plus important et que l'on retrouve massivement dans les smartphones, montres connectés ...

TABLE II. COMPARISON OF WIRELESS TECHNOLOGIES FOR HOME AUTOMATION

Indices	<i>ZigBee</i>	<i>Z-Wave</i>	<i>Wi-Fi</i>	<i>Bluetooth</i>
Power consumption	100 mw	1 mw	High	10 mw
Range	100 m	30 m	1000 m	10 m
Cost	Low	High	Medium	Very low
Scalability	6000	> 6000	32	20
Interoperability	Same manufacturer	Different manufacturers	Wi-Fi compatible devices	Bluetooth compatible devices

Figure 6 Comparaison des technologies

Ces appareils communiquent ensuite avec des applications ou des solutions permettant à l'utilisateur d'avoir accès à son statut ou contrôler l'appareil par exemple, pour les particuliers, on connaît Google Home, Amazon Alexa, Apple HomeKit, Tuya, Philips HUE qui permettent le contrôle depuis des smartphones, enceintes ou écrans connectés et dans les entreprises directement dans des applications métiers comme SAP, Oracle IoT, Cisco IoT Control Center, AWS IoT ou encore Google Cloud IoT.

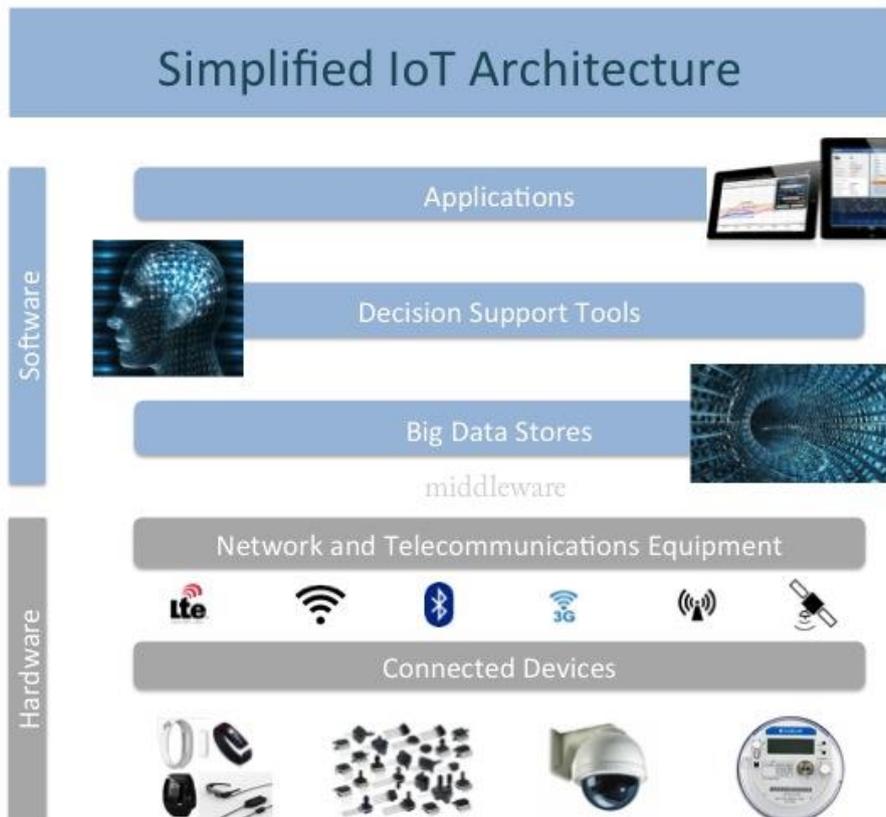


Figure 7 Classical IoT Architecture (Lefrançois)

Des solutions adaptables ont vu aussi le jour avec par exemple le Raspberry Pi, l'Arduino... Des mini-ordinateurs, auquel on peut associer de nombreux capteurs.

La société américaine iPourIt utilise, par exemple, un Raspberry Pi sur ses machines à bière afin de contrôler l'âge des consommateurs par RFID et vérifier le niveau des tireuses à l'aide de capteurs. Ces solutions adaptables, facilement maintenables et ouvertes ont permis de contribuer à la popularité de ces objets et à la réduction des coûts (Raspberry Pi computers have allowed this company to reduce the acquisition cost for its operators, 2022).

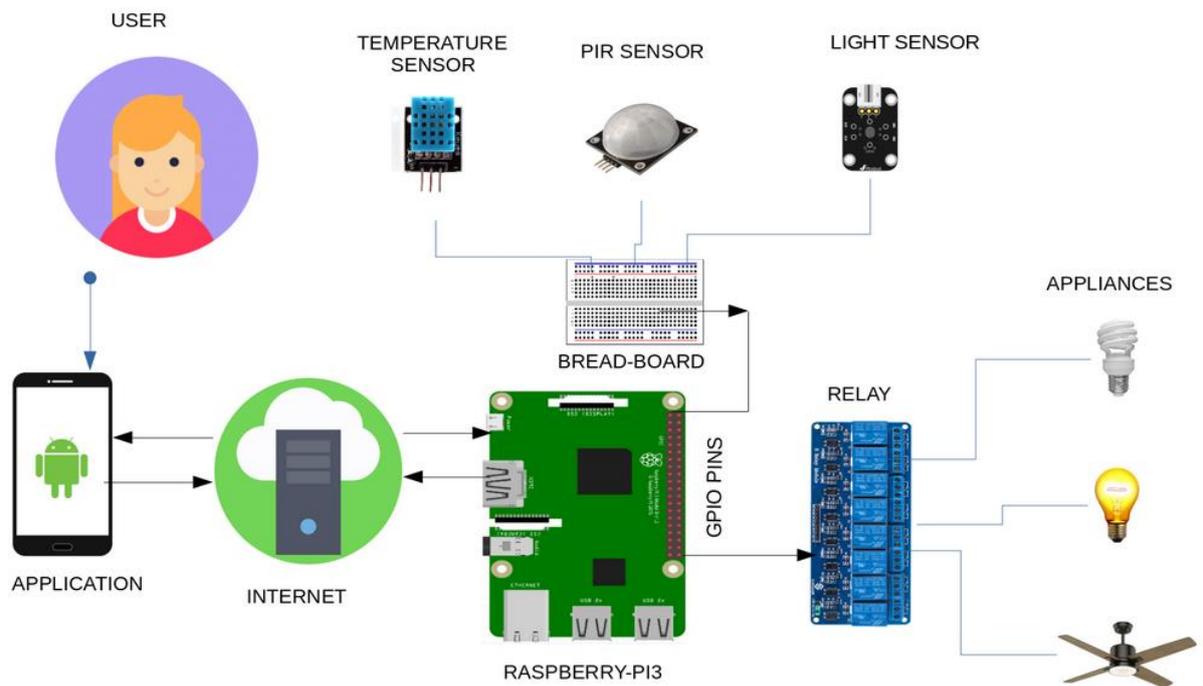


Figure 8 Exemple internet des objets avec Raspberry Pi

Des systèmes d'exploitation dédiés à ces solutions ont aussi vu le jour avec par exemple Windows 10 IoT (Microsoft), Tyzen (Samsung), TinyOS, FreeRTOS (Amazon). On utilise souvent des systèmes RTOS (Real Time Operating System) qui permettent de focaliser les processus sur leurs tâches et de définir le temps entre le stimulus et la réponse de sortie.

Sur un point technologique les évolutions ont été nombreuses, un temps anarchique elles se stabilisent et offrent un éventail de matériels et systèmes pour répondre à tous les besoins.

Cependant elles ont longtemps souffert d'un défaut de standardisation avec chaque marque qui ont développé leurs propres solutions, connectivités et appareils amenant à une complexification de l'interopérabilité, un défaut d'harmonisation des protocoles et des problèmes de sécurité.

4 Main Appliances of IoT Standards



*The copyright of trademarks quote in the news belonged to the related companies
Source: Institute for Information Industry 2015/05*

Figure 9 Les différents standards

Ces différents standards se sont unis, pour la plupart, autour d'un seul au sein de la Connectivity Standards Alliance avec Matter qui va permettre d'avoir un vrai modèle de connectivité et d'interopérabilité entre les différents acteurs (Amazon, Apple, Google, Huawei, Zigbee Alliance), les premiers appareils utilisant ce système devraient être disponibles à partir de 2022 (Matter).

3.6 SÉCURITÉ ET PROTECTION DE LA VIE PRIVÉE

Les deux grandes problématiques liées à l'internet des objets sont la sécurité de ces objets ainsi que les risques pour la vie privée.

La multiplication des différentes technologies et la présence de ces appareils tout autour de nous ont mené à des problèmes de sécurisation du fait d'appareil non mis à jour, non sécurisés ou volontairement « curieux ».

En 2016, le logiciel malveillant Mirai s'est répandu de façon massive sur l'internet des objets en utilisant des appareils obsolètes et mal sécurisés afin de mener de nombreuses attaques DDoS (Understanding the Mirai Botnet, 2017) vers de grands groupes (OVH, Netflix, Github ...).

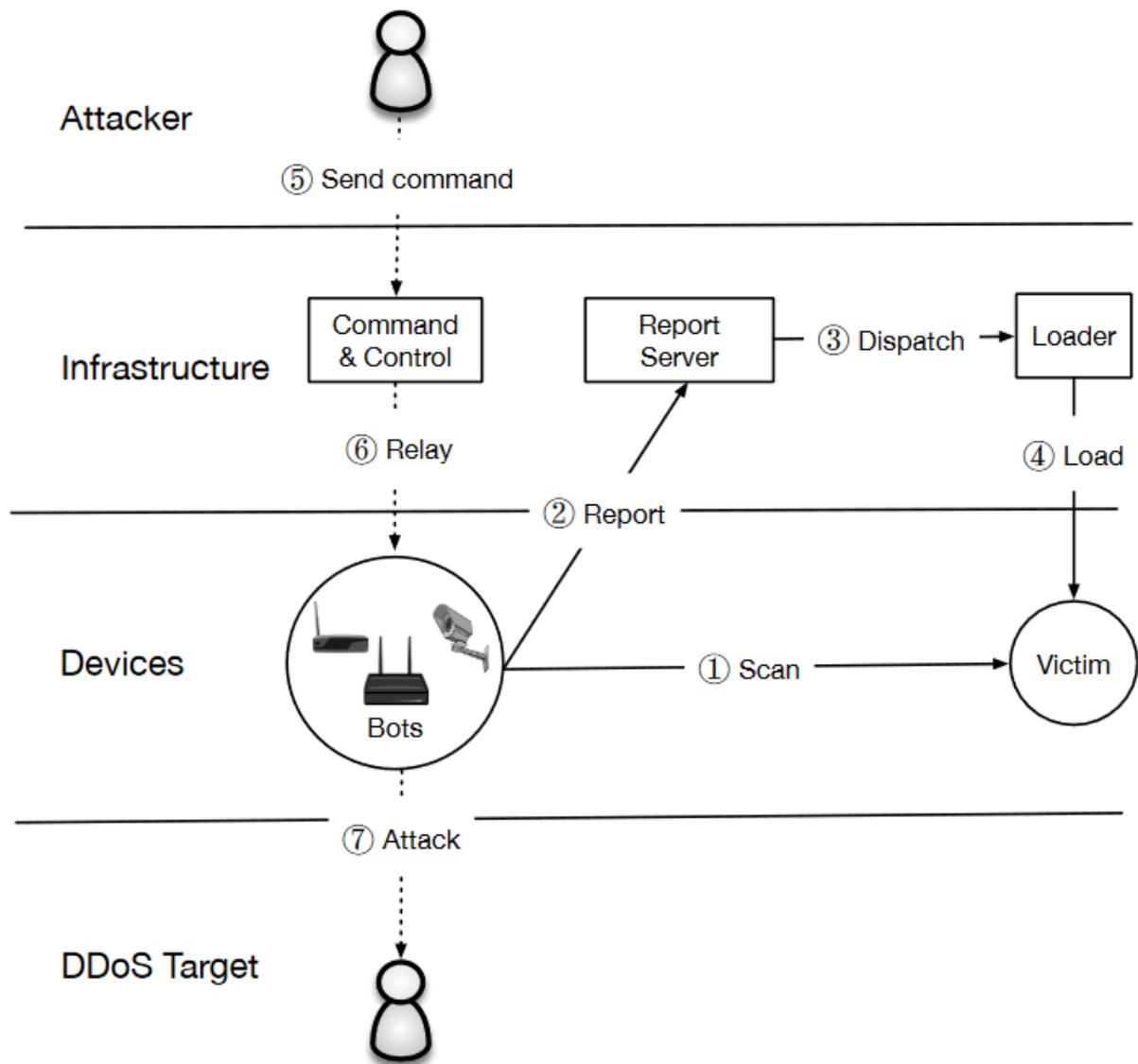


Figure 10 Exemple d'une attaque venant d'un bot

Bien que de nombreux appareils ont été mis à jour la question se pose pour les autres : comment protéger les infrastructures de ces appareils ? La solution a été, dans ce cas, de mettre en place des solutions pour détecter ces attaques en identifiant et analysant le comportement de celles-ci.

Un autre sujet est celui de la confidentialité, l'affaire VTech est un exemple de ces problèmes avec des millions de données d'objets connectés qui étaient stockés sur des serveurs non sécurisés : des identifiants jusqu'aux photos prises par ces jouets (Les données de 6,4 millions d'enfants piratées depuis le site du fabricant de jouets VTech, 2015) ont pu être obtenus par les attaquants.

L'internet des objets est aussi, par exemple, considérablement utilisé en Chine pour surveiller la population (Louvet, 2020) via des puces, smartphones, caméras... Le pays est aussi la cible de sanctions pour avoir mis en place des solutions permettant d'avoir des « portes ouvertes » sur des appareils vendus partout dans le monde (6 questions pour comprendre les accusations d'espionnage contre Huawei, 2019).

Des schémas de sécurisation pour les entreprises se mettent en place afin de sécuriser, prévenir et détecter les menaces (Charles Wheelus, 2020).

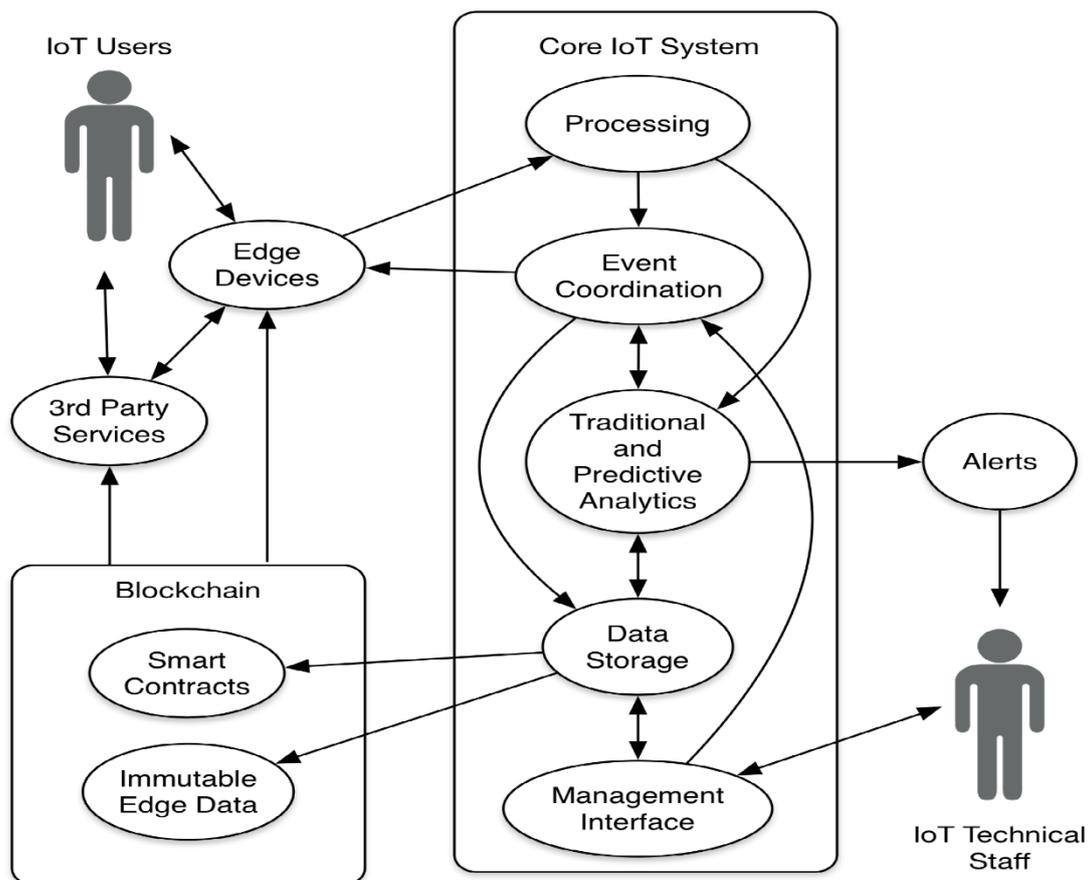


Figure 11 Exemple de modèle de sécurisation

4 TRAVAIL HYBRIDE

4.1 DÉFINITION DU TRAVAIL HYBRIDE

Le travail hybride est le fait de travailler depuis d'autres emplacements que l'entreprise, on parle couramment de télétravail mais il y a aussi les espaces de coworking (espaces de travail partagés où des personnes travaillant dans différents secteurs se retrouvent) ainsi que par exemple les transports, des résidences temporaires... Et qui amène à des usages différents tel que les conférences vidéo, l'utilisation du cloud et autres applications pour le partage.



Figure 12 Illustration travail hybride

4.2 HISTOIRE ET ÉVOLUTIONS

Avec le développement d'internet, de nombreuses applications métiers, qui étaient auparavant installées localement sur les postes, ont migré vers des serveurs privés puis vers des solutions totalement web via le cloud, on peut prendre, par exemple, le simple exemple de la suite bureautique Microsoft Office qui, à l'origine, fonctionnait uniquement en local et fonctionne maintenant, en grande majorité, en mode « service » accessible depuis

n'importe quel poste, de même pour les fichiers avec les systèmes de stockage en ligne (One Drive, Google Drive, Share Point ...).

Ces évolutions ont permis et favorisé le développement du travail en dehors de l'entreprise, on peut maintenant, tant avec les évolutions technologiques (débit, vidéo, appareils mobiles ...) qu'avec les nouvelles solutions créées pour le travail collaboratif (Teams, Slack ...), travailler de la même manière au sein de l'entreprise que dans un autre lieu extérieur.

En 12 ans le nombre de personnes travaillant à distance a cru de 159%, la croissance est constante et peut apporter des bénéfices autant pour les employés que pour les entreprises.

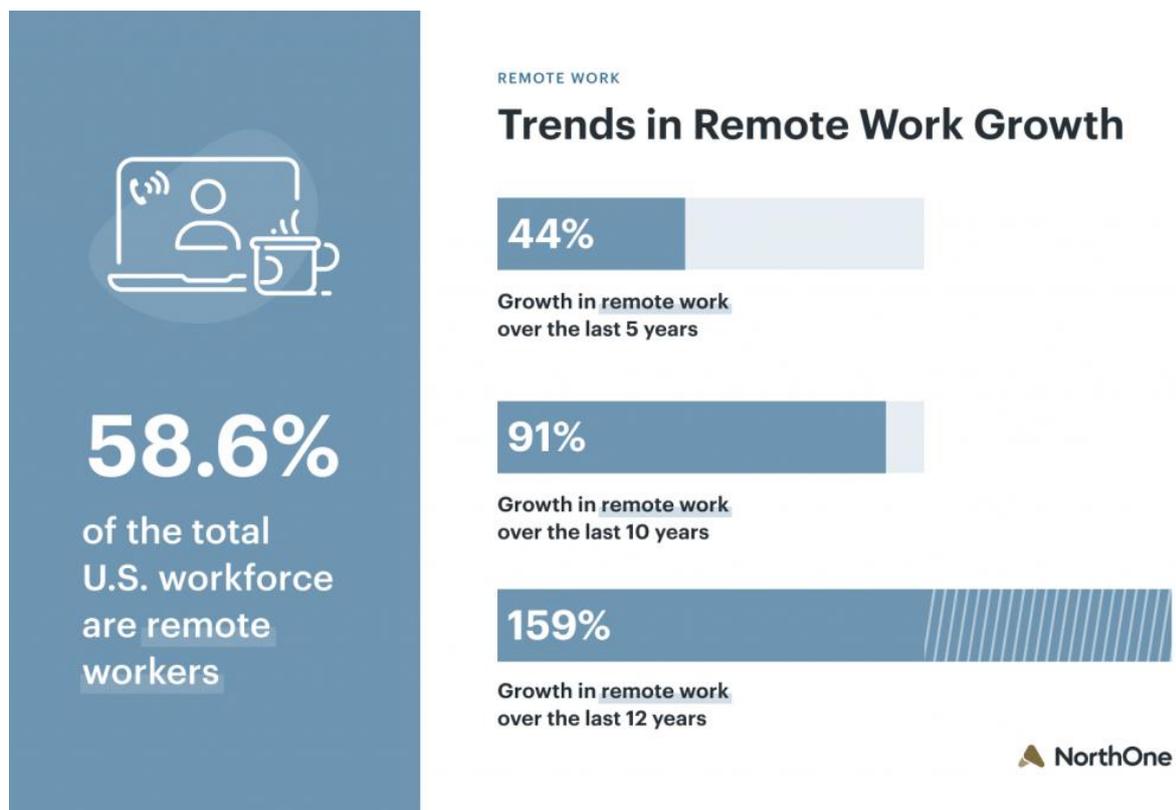


Figure 13 Remote Work Statistics (12 Remote Work Statistics to Know in 2022, 2022)

4.3 LA TENDANCE « FLEX OFFICE »

On utilise maintenant souvent le terme de « Flex Office », la première entreprise à avoir mis en place ce système à grande échelle pour l'ensemble des employés est Andersen Consulting (maintenant Accenture) en 1995, ça se traduisait par un environnement sans bureau attribué, disponible sur réservation, reprenant le principe de l'hôtellerie avec des services (Andersen Consulting inaugure le bureau à temps partagé, 1995). Cela permet un gain économique du fait de ne pas avoir des bureaux inoccupés mais ça a aussi un impact psychologique.

Maintenant il s'applique à de nombreuses entreprises et s'est étendu aussi vers des structures externes dites de « espaces de coworking » qui permettent de louer un bureau pour travailler avec des personnes d'autres entreprises dans un cadre adapté (bureau, connexion, salle de réunion, café, imprimante ...).



Figure 14 Espace coworking 144 à Nantes

4.4 PANDÉMIE DE COVID 2019

La pandémie de coronavirus qui a sévi dans le monde à partir du début de l'année 2020 a poussé à la mise en place de confinements et de restrictions de déplacement et a engendré une hausse massive du recours au télétravail,

celui-ci a même été imposé dans certaines entreprises, à l'heure actuelle il n'est plus obligatoire depuis le 14 mars 2022.

Ces changements pourraient perdurer, on voit notamment que les tranches qui avaient 1 à 2 jours ont diminué et une explosion de la tendance pour les valeurs supérieures.

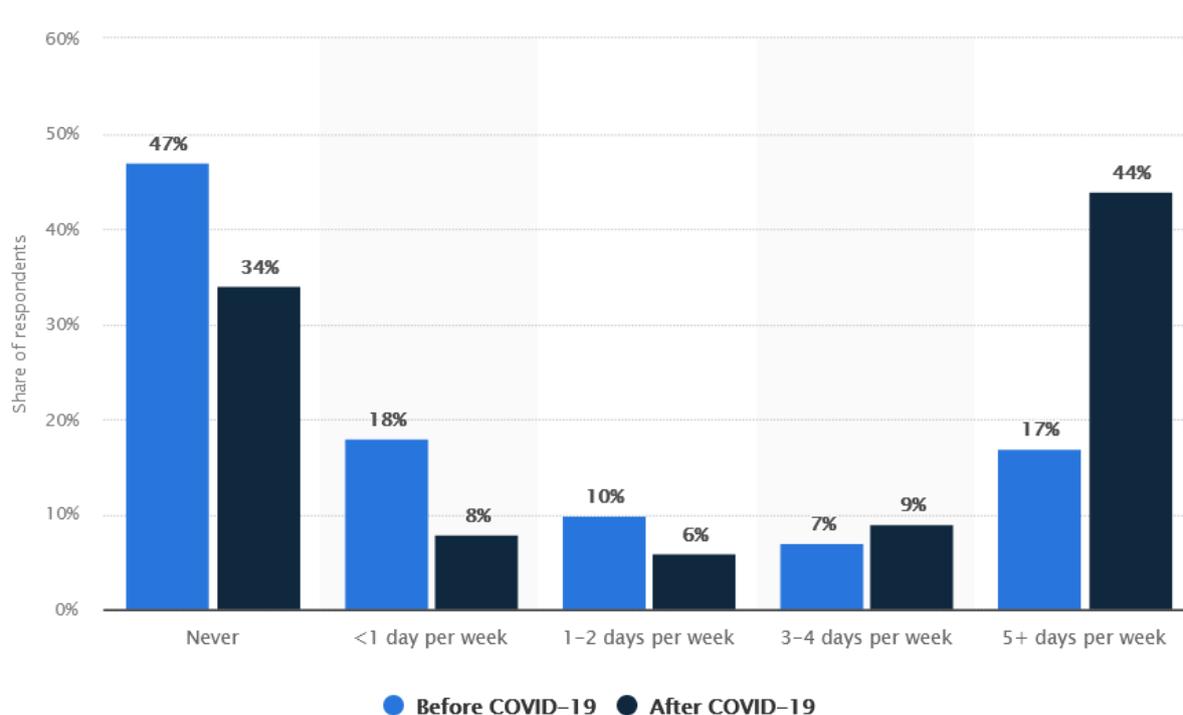


Figure 15 Statistiques télétravail avant et après covid

La pandémie a aussi révélé l'impact technologique d'un passage massif au télétravail avec une surcharge des connexions et des incidents à répétitions n'épargnant pas les grandes plateformes qui ont dû mettre en place des stratégies pour alléger les flux.

4.5 SÉCURISATION ET RISQUES

La sécurisation des outils utilisés en dehors de l'entreprise est primordiale, l'utilisation de VPN est répandue pour accéder aux ressources internes des entreprises mais elle permet aussi aux attaquants d'y accéder, de même qu'un poste de travail peut se connecter via des accès non sécurisés (wifi public,

routeur mal configuré ...), on ne compte plus les découvertes de failles (protocole WPS compromis, accès à des administrations de routeur via des mots de passe basiques ...).

Les attaques sur les infrastructures se sont produites régulièrement pendant la pandémie du fait de l'impréparation de certaines entreprises et de la précipitation qu'imposait la situation, de nombreuses ouvertures de flux ont été mises en place, afin de permettre le travail depuis l'extérieur, ouvrant un boulevard aux pirates avec des postes non mis à jour et des identifications trop simplistes.

Dès le début de la pandémie la Métropole Aix-Marseille Provence a été par exemple l'objet d'une importante attaque menant à l'arrêt de l'ensemble de ses serveurs (Koudjih, 2020), de même que de nombreuses entreprises et administrations pendant cette période (Nabe).

Ces attaques ont utilisé des méthodes traditionnelles (hameçonnage, logiciel malveillant ...) mais aussi de nouvelles méthodes, par exemple, en passant par les réseaux sociaux ou les applications de collaboration.

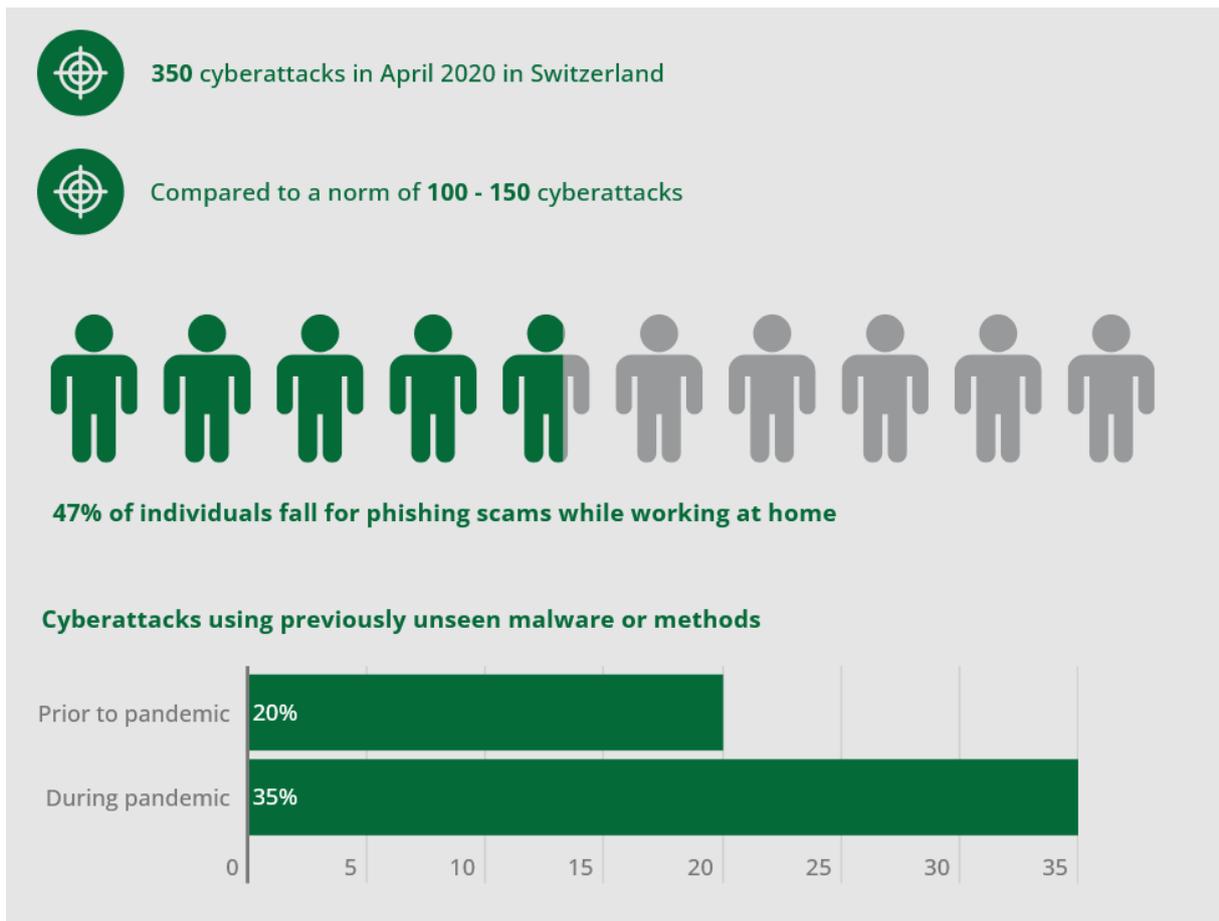


Figure 16 Cyberattaques pendant la pandémie de Covid en Suisse (Deloitte)

4.6 LES CHIFFRES EN FRANCE

En France le travail hybride progresse doucement, même après la pandémie, les chiffres se stabilisent à, en moyenne, 2 jours par semaine.

Le rythme moyen du télétravail est d'environ **2 jours par semaine**

Base
Salariés

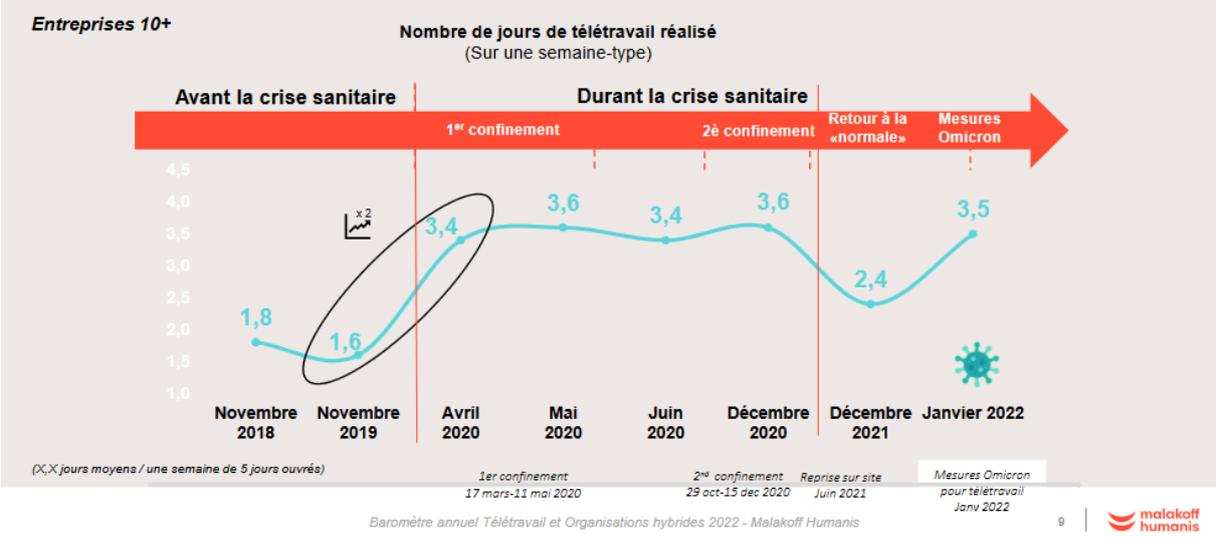


Figure 17 Jours de télétravail en France selon la période

Les managers sont toujours, pour moitié, réticents à ce mode de travail (Baromètre annuel Télétravail et Organisations Hybrides 2022, 2022) du fait de manque de cohésion et de travail d'équipe.

Les entreprises doivent aussi s'adapter pour proposer un management différent et mettre en place, de façon pérenne, des process adaptés au travail hybride (flexibilité, sécurité, organisation ...).

Les salariés eux sont plutôt favorables à un mix entre les deux.

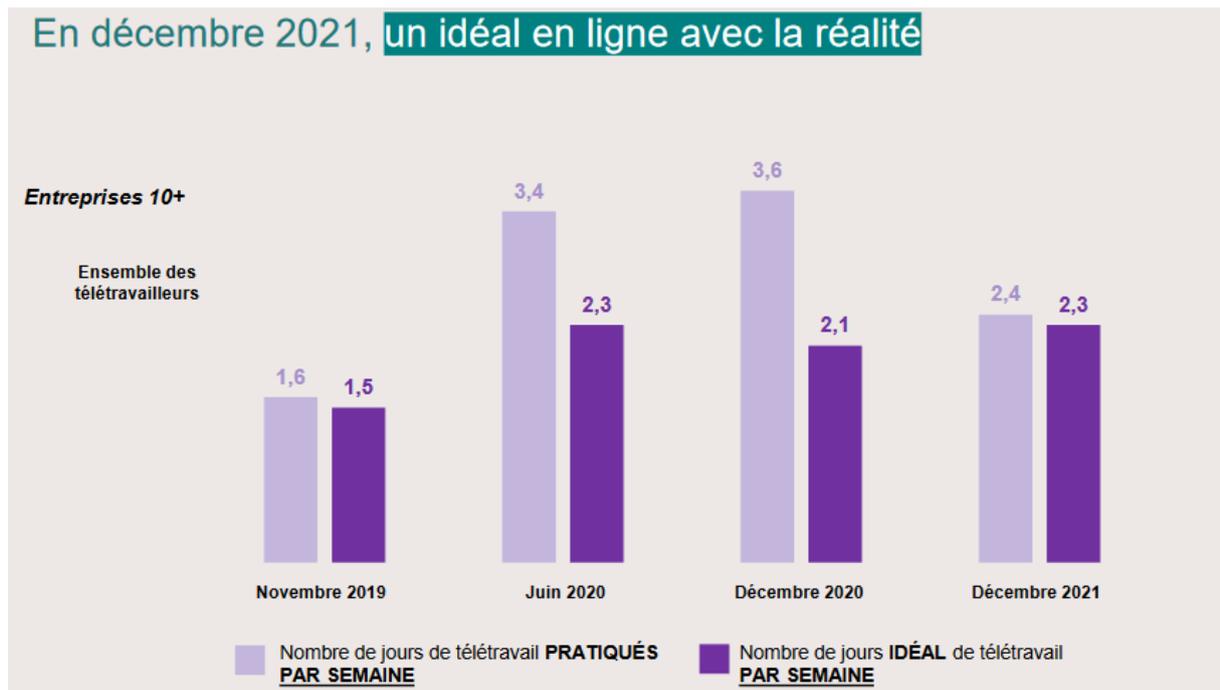


Figure 18 Nombre de jours pratiqué et nombre de jour idéal

Au niveau des syndicats des problématiques remontent souvent autour de la prise en charge des frais engendrés, certaines entreprises indemnisant le strict minimum aux alentours de 10 euros par mois alors que les frais sont plus importants, et militent aussi pour une redistribution des économies engendrées.

4.7 CONSÉQUENCES PSYCHOLOGIQUES ET CULTURE D'ENTREPRISE

Détresse psychologique, sentiment de solitude, perte de la culture d'entreprise... Bien que le travail hybride apporte des avantages pour la vie personnelle, en permettant d'avoir une gestion plus libre, moins de contraintes sur les trajets et une diminution du stress, certaines personnes ne s'y retrouvent pas du fait de l'isolement, du manque d'interactions et de la déshumanisation des espaces de travail (bureau non attribué, ne pas savoir avec qui on va travailler à côté de nous ...).

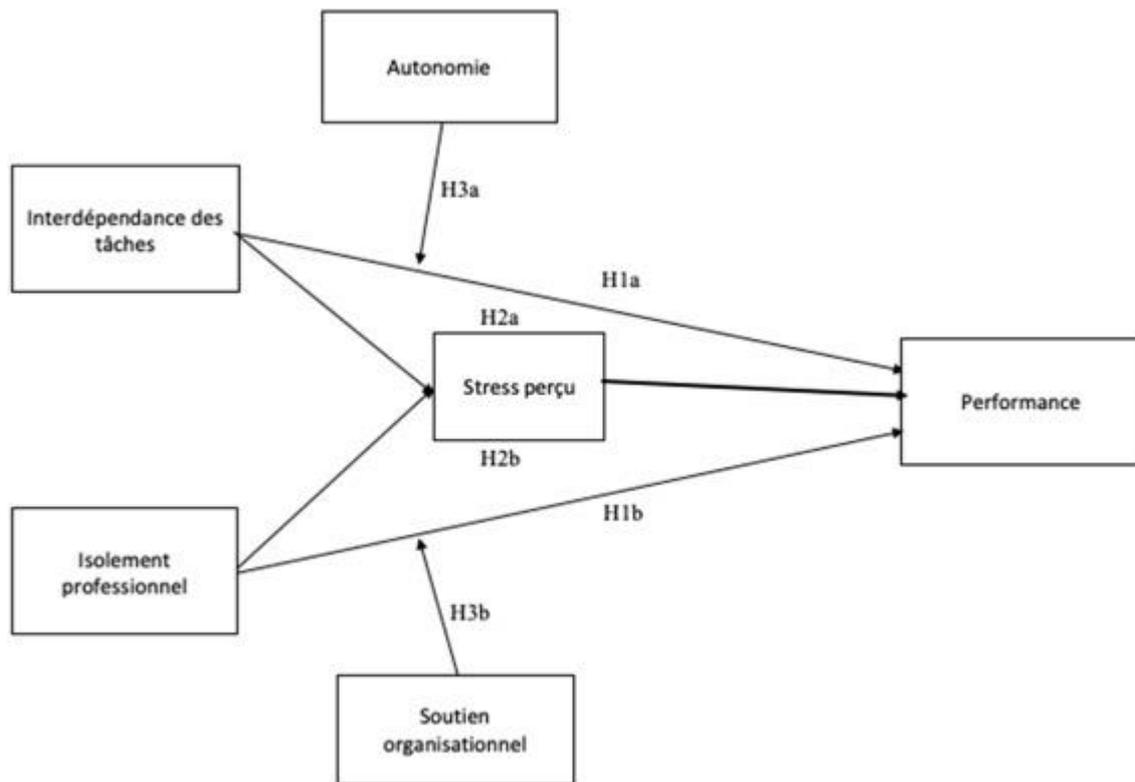


Figure 19 Modèle théorique (J.F.R.Registre, 2022)

La culture d'entreprise aussi se voit changée, moins de personnes participent aux événements et le sentiment d'appartenance au collectif diminue, ce constat vient aussi grandement du fait de l'impréparation des entreprises, des solutions sont à mettre en place afin de repenser l'organisation et passer par des outils permettant une meilleure communication et des interactions entre les collaborateurs.

5 L'ÉMERGENCE DU « SMART OFFICE »

Le terme « Smart Office » est une évolution du terme « Flex Office », il intègre les avantages de l'internet des objets pour améliorer le travail hybride et la gestion de celui-ci et aussi des applications permettant le travail collaboratif à distance (Office 365, Google Workspace ...).

Il permet de mettre en place un environnement « à la demande » permettant de contrôler l'occupation, la consommation électrique et l'accès aux ressources.

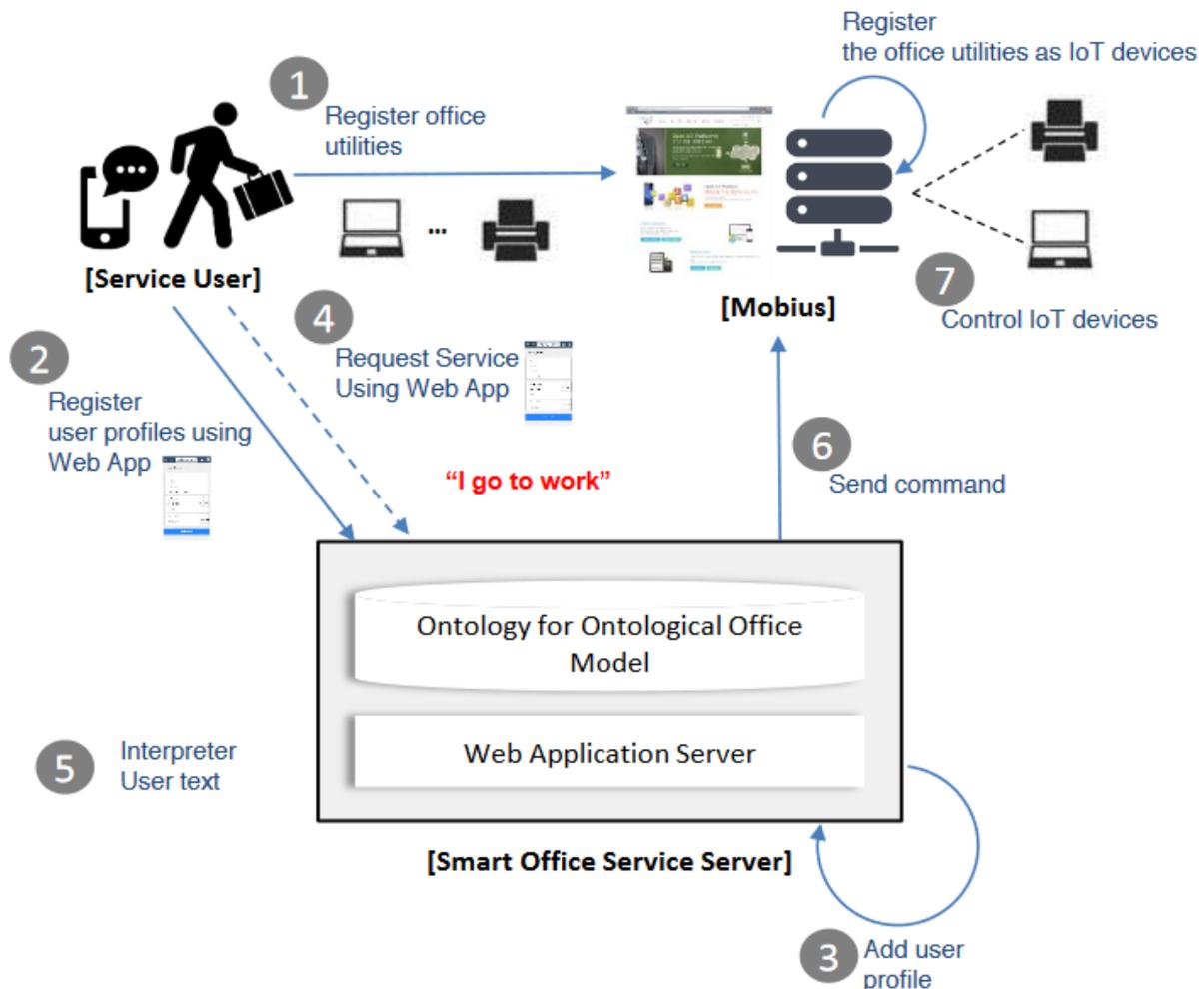


Figure 20 Exemple de workflow en smart office (Minwoo Ryu, 2015)

C'est sans doute vers ça que nous nous dirigeons naturellement avec les évolutions technologiques et notre monde de plus en plus connecté.

Des entreprises se spécialisent dans ces solutions avec des gestions poussées des accès, casiers, cartographie interactive, réservations des espaces, cantine, contrôles de l'environnement, capteurs telles que les sociétés [Welcomr](#) ou [GoBright](#).

Cette évolution est aussi plus globale avec des villes de plus en plus connectées avec le concept de « Smart City ».



Figure 21 Schéma d'une smart city (Global Smart City, 2018)

6 IMPACT ÉCOLOGIQUE ET EFFET REBOND

Contrairement à l'idée que l'on pourrait se faire, le travail hybride ne réduit pas automatiquement l'empreinte écologique, bien que nous utilisions moins notre véhicule il accroît les dépenses de chauffage, climatisation, lumière, matériel électronique ... Et du fait de l'éloignement voulu par certains employés avec cette possibilité même les trajets deviennent autant consommateur (ADEME, 2021) voir plus. On parle alors d'effet rebond (Jevons, 1865), le bénéfice apporté par l'amélioration d'un facteur amène en fait une augmentation globale supérieure par l'ensemble des autres facteurs.

Dans le cas du travail hybride, s'il est bien mené, il peut devenir intéressant dans le cas des entreprises ayant vraiment mis en place un système de « Flex Office » via, par exemple, le « smart office » permettant d'optimiser l'espace de travail et réduire la consommation des bureaux voir même, au travers des postes de

travail, de réduire la consommation de chaque ordinateur en passant par de la virtualisation pour une utilisation des ressources adaptative.

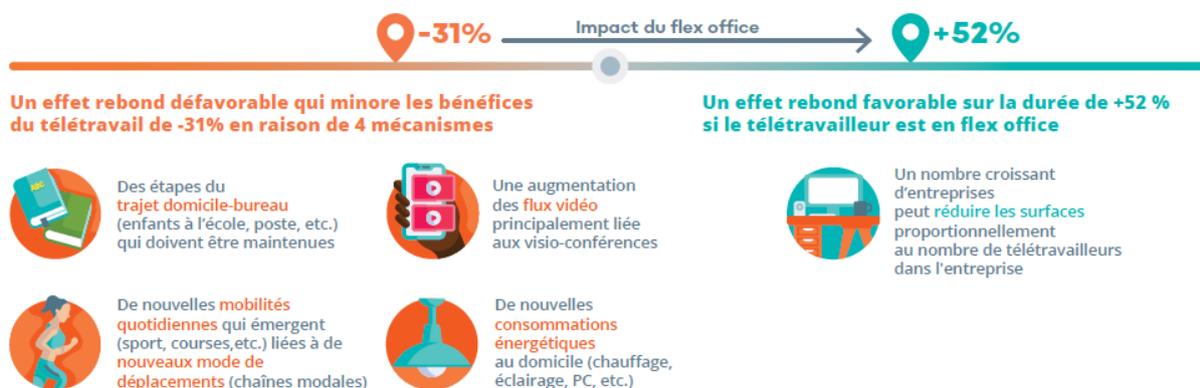
LE TÉLÉTRAVAIL, VRAIMENT BON POUR L'ENVIRONNEMENT ?

UNE RÉDUCTION DES TRAJETS PENDULAIRES DOMICILE - TRAVAIL TRÈS BÉNÉFIQUE...



... MODULÉE PAR DES EFFETS REBOND SIGNIFICATIFS FAVORABLES ET DÉFAVORABLES ...

Les effets rebond sont les mécanismes induits par le télétravail par lesquels son bénéfice environnemental est minoré ou majoré



DE NOUVEAUX EFFETS REBOND SYSTÉMIQUES OU DE LONG TERME À ÉVALUER ET SUIVRE



greenworking

Figure 22 Infographie impact du télétravail

L'internet des objets a, pour sa part, déjà prouvé son efficacité sur les économies d'énergie au travers, par exemple, des thermostats connectés qui programment « intelligemment » la température intérieure en adéquation avec les données météo cependant la multiplication de ces objets apporte aussi une consommation plus importante, certaines voitures, par exemple, embarquent des technologies équivalentes à un ordinateur.

Les bénéfices sont aussi non négligeables dans la gestion urbaine avec des communes qui mettent en place des solutions intelligentes de gestion de

l'éclairage public (Dalmaz-Nicolas, 2022), on peut aussi suivre ses consommations avec les compteurs Linky et Gazpar afin de détecter une surconsommation.

7 CONCLUSION

L'internet des objets révolutionne notre quotidien, de la même manière qu'il peut apporter des solutions à la maison il permet aussi améliorer la gestion du travail hybride.

Les entreprises se lancent déjà dans ces outils pour faciliter l'organisation : réserver une salle de réunion avec un simple QR code, badger pour ouvrir un véhicule, économiser l'électricité sur les espaces non utilisés... Mais il y aussi des dérives et des problèmes de sécurité et de confidentialité à ne pas négliger.

Il y a quelques années certains masquaient leur webcam avec un bout de scotch mais que faire avec tous les appareils qui nous entourent désormais et qui sont liés à internet ? Certaines enceintes proposent de couper physiquement l'accès au micro mais avec la multiplicité des appareils nous allons sans doute voir émerger de nouvelles formes d'espionnage visant ces objets et permettant de suivre nos actions, nous écouter et nous observer.

Ces solutions nécessitent une vraie réflexion sur leurs mises en place ainsi que sur leurs impacts, l'humain ne se gère pas comme une machine.

Nous n'en sommes qu'au début, la volonté de flexibilité du travail est très présente chez les employés mais celle-ci nécessite une adaptation des entreprises tant au niveau technologique qu'au niveau organisationnel afin d'apporter des solutions durables et d'amener à une véritable transformation structurelle de nos modes de travail.

8 BIBLIOGRAPHIE

12 Remote Work Statistics to Know in 2022. (2022). Récupéré sur Northone:
<https://www.northone.com/blog/small-business/remote-work-statistics>

6 questions pour comprendre les accusations d'espionnage contre Huawei .
(2019). Récupéré sur Le Monde:
https://www.lemonde.fr/pixels/article/2019/05/22/espionnage-queelles-sont-les-accusations-contre-le-geant-chinois-huawei_5465556_4408996.html

ADEME. (2021). *Caractérisation des effets rebond induits par le télétravail*.
Récupéré sur <https://librairie.ademe.fr/mobilite-et-transport/3776-caracterisation-des-effets-rebond-induits-par-le-teletravail.html>

Andersen Consulting inaugure le bureau à temps partagé. (1995). Récupéré
sur Les Echos: <https://www.lesechos.fr/1995/11/andersen-consulting-inaugure-le-bureau-a-temps-partage-870225>

Baromètre annuel Télétravail et Organisations Hybrides 2022. (2022). Récupéré
sur Malakoff Humanis:
<https://newsroom.malakoffhumanis.com/assets/2022-02-24-malakoffhumanis-etude-teletravail-organisations-hybrides-presse-newsroom-ppt-pdf-fd89-63a59.html?lang=fr>

Carnot, I. (2011). *Le livre blanc : Objets communicants et Internet des objets*.
Récupéré sur https://www.instituts-carnot.eu/sites/default/files/images/AiCarnot-Livre_Blanc-Objets_CommunicantsetInternet_des_Objets-long.pdf

Charles Wheelus, X. Z. (2020). *IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework* . Récupéré sur MIRI:
<https://www.mdpi.com/2624-831X/1/2/16/htm>

Dalmaz-Nicolas, V. (2022). *Dans le Calvados, la commune d'Épron expérimente l'éclairage public à la demande* . Récupéré sur France info:
<https://www.francetvinfo.fr/economie/energie/dans-le-calvados-la->

commune-depron-experimente-leclairage-public-a-la-
demande_5063602.html

Global Smart City. (2018). Récupéré sur Internet of Business: <https://internetofbusiness.com/global-smart-city-platform-market/>

Illa, P. K. (2018). *Practical Guide to Smart Factory Transition Using IoT, Big Data and Edge Analytics*. Récupéré sur IEEE: <https://ieeexplore.ieee.org/abstract/document/8478188/figures#figures>

J.F.R.Registre. (2022). *Effet du télétravail sur la santé psychologique et la performance des travailleurs durant la pandémie de la Covid-19*. Récupéré sur Science Direct.

Jevons, W. S. (1865). *Paradoxe de Jevons*. Récupéré sur Wikipédia: https://fr.wikipedia.org/wiki/Paradoxe_de_Jevons

Koudjih, S. (2020). *Ransomware: Cyberattaque de grande ampleur à la Métropole Aix-Marseille-Provence*. Récupéré sur IDNA: <https://www.idna.fr/2020/12/21/ransomware/>

Lefrançois, M. (s.d.). *Introduction to the Internet-of-things*. Récupéré sur MINES St Etienne: <https://ci.mines-stetienne.fr/teaching/maj-info/iot/2017/1/>

Les données de 6,4 millions d'enfants piratées depuis le site du fabricant de jouets VTech. (2015). Récupéré sur Usine Digitale: <https://www.usine-digitale.fr/article/les-donnees-de-6-4-millions-d-enfants-piratees-depuis-le-site-du-fabricant-de-jouets-vtech.N367457>

Louvet, S. (2020). *Arte « Tous surveillés, 7 milliards de suspects »*. Récupéré sur https://boutique.arte.tv/detail/tous_surveilles_7_milliards_de_suspects

Matter. (s.d.). Récupéré sur Connectivity Standards Alliance: <https://csa-iot.org/all-solutions/matter/>

Minwoo Ryu, J. K. (2015). *Integrated Semantics Service Platform for the Internet of Things: A Case Study of a Smart Office*. Récupéré sur MDPI: https://mdpi-res.com/d_attachment/sensors/sensors-15-02137/article_deploy/sensors-15-02137.pdf?version=1421660413

- Nabe, C. (s.d.). *Impact of COVID-19 on digital working and cybersecurity*.
Récupéré sur <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html>.
- Nayak, S. (2021). *A Review on Edge Analytics: Issues, Challenges, Opportunities, Promises, Future*. Récupéré sur ARXIV Cornell University: A Review on Edge Analytics: Issues, Challenges, Opportunities, Promises, Future
- Quelle gouvernance pour l'IoT ? . (s.d.). Récupéré sur <https://www.futuribles.com/fr/groupe/iot-2025/document/quelle-gouvernance-pour-liot/>
- Raspberry Pi computers have allowed this company to reduce the acquisition cost for its operators.* (2022). Récupéré sur Raspberry Pi: <https://www.raspberrypi.com/success-stories/ipourit/>
- Society : Build digital democracy* . (2015). Récupéré sur <https://www.nature.com/articles/527033a>
- Somayya Madakam, R. R. (s.d.). *Internet of Things (IoT) : A Literature Review* : . Récupéré sur Scientist Research: https://www.scirp.org/html/56616_56616.htm?pagespeed=noscript
- télécommunications, U. i. (2012). *ITU-T Recommendations*. Récupéré sur <https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=11559&lang=fr>.
- Understanding the Mirai Botnet.* (2017). Récupéré sur USENIX: <https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis>
- Université Carnegie Mellon (Pittsburgh, P. E.-U. (1982). *La machine à soda connectée à internet : The "Only" Coke Machine on the Internet*. Récupéré sur https://www.cs.cmu.edu/~coke/history_long.txt

9 ILLUSTRATIONS

Figure 1 Machine à soda connectée	3
Figure 2 Exemples de l'internet des objets	4
Figure 3 Le livre blanc : Objets communicants et Internet des objets (Carnot, 2011)	5
Figure 4 Exemple de schéma dans une usine (Illa, 2018)	6
Figure 5 Edge analytics et Big data (Nayak, 2021)	7
Figure 6 Comparaison des technologies	8
Figure 7 Classical IoT Architecture (Lefrançois)	9
Figure 8 Exemple internet des objets avec Raspberry Pi	10
Figure 9 Les différents standards	11
Figure 10 Exemple d'une attaque venant d'un bot.....	12
Figure 11 Exemple de modèle de sécurisation	13
Figure 12 Illustration travail hybride.....	14
Figure 13 Remote Work Statistics (12 Remote Work Statistics to Know in 2022, 2022)	15
Figure 14 Espace coworking 144 à Nantes.....	16
Figure 15 Statistiques télétravail avant et après covid.....	17
Figure 16 Cyberattaques pendant la pandémie de Covid en Suisse (Deloitte)	19
Figure 17 Jours de télétravail en France selon la période	20
Figure 18 Nombre de jours pratiqué et nombre de jour idéal.....	21
Figure 19 Modèle théorique (J.F.R.Registre, 2022)	22
Figure 20 Exemple de workflow en smart office (Minwoo Ryu, 2015)	23

Figure 21 Schéma d'une smart city (Global Smart City, 2018)	24
Figure 22 Infographie impact du télétravail.....	25