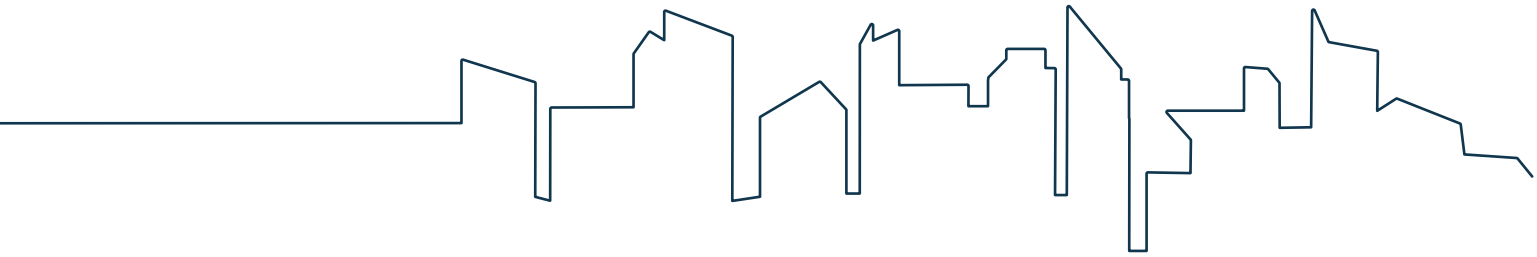
EGE Ecole de Guerre Economique



SMART CITY : ENJEUX CYBERDEFENSE ET CYBER-RESILIENCE

Inasse BOUALLEGUE - Roland FRIEH - Vincent HAUTOT - Yves HOUSSOU

Sébastien AUTHIER - Ruslans SENKOVICS - Ignace AHITCHEME

24 Mai 2021

Promotion Executive MBA MRSIC07

SOMMAIRE

INTRODUCTION

En 2008, pour la première fois dans l'histoire de l'humanité, il y avait plus de citadins que de ruraux, et les tendances montrent que ce phénomène n'est pas près de s'inverser. Les Nations unies estiment que d'ici à 2030, plus de 60 % de la population mondiale vivra dans des "mégapoles" (10 millions), des grandes (5-10 millions), des moyennes (1-5 millions), des petites villes et des communautés périurbaines, de plus en plus concentrées en Asie, en Afrique et en Amérique latine.

Les derniers rapports du Groupe d'Experts Intergouvernemental sur l'Évolution du Climat (GIEC) sur les établissements humains, les infrastructures et l'aménagement du territoire indiquent que l'expansion des zones urbaines (centres urbains et banlieues) est en moyenne deux fois plus rapide que la croissance de la population urbaine, et que la croissance prévue au cours des trois premières décennies du XXIe siècle sera plus importante que l'expansion urbaine cumulée de toute l'histoire de l'humanité.

Cette urbanisation rapide est accompagnée de l'augmentation de la demande d'énergie, d'eau et de services sanitaires, ainsi que des services tels que l'éducation et les soins de santé. D'où la nécessité d'utiliser des ressources efficacement et de développer une ville "durable et intelligente" pour répondre aux besoins des habitants. En réponse à ces besoins, il existe actuellement des centaines de projets de ville intelligentes dans le monde entier, à la fois dans les pays développés et en développement. Les exemples abondent, comme Amsterdam, Barcelone, Paris, Oslo, San Francisco, Santander, Londres, Singapour, Tianjin. Ce phénomène peut contribuer à une meilleure gouvernance et à une gestion efficace des infrastructures telles que l'eau, l'énergie, le transport et les maisons, ainsi qu'une meilleure qualité de vie.

Le programme 2030 pour le développement durable, et l'accord de Paris dans le cadre de la convention sur les changements climatiques constituent un contexte propice des agendas pour aborder ce thème prioritaire. Les villes et les infrastructures urbaines vont dominer la majorité du développement humain dans un futur prévisible et la science, la technologie et l'innovation, y compris les technologies de l'information et de la communication (TIC), peuvent leur permettre de développer des habitats plus intelligents et plus propres. En corollaire, les villes peuvent être planifiées, conçues, construites et exploitées de manière plus holistique en

tant que sphère d'influence du pouvoir politique, du commerce, de l'éducation et de l'innovation, avec un énorme potentiel pour répondre aux besoins du développement durable.

Les concepteurs de villes intelligentes utilisent des technologies modernes telles que l'informatique dans les nuages, l'Internet des objets, les réseaux de communication (Wi-Fi, 5G, RFID, etc.), les capteurs et les technologies d'apprentissage automatique pour permettre aux différents composants des villes intelligentes de coopérer et d'interagir avec l'architecture en réseau. La complexité inhérente et les nouvelles méthodes d'interaction avec les citoyens requises pour la modification des infrastructures existantes mettent en évidence les défis politiques, réglementaires et techniques importantes pour les gouvernements et les collectivités. L'un des principaux défis du développement des villes intelligentes est la sécurité, la résilience des infrastructures des villes et de la gouvernance des données. Cela concerne les données déjà présentes dans les bases de données de la ville, mais aussi la mise en relation des données avec les nouveaux systèmes et capteurs présents dans la ville intelligente, qui ont un impact sur la sécurité et la vie privée des citoyens. Les menaces découlant de la sécurité de l'information, de la confidentialité des données et des facteurs liés à la cybernétique, où l'accès non autorisé à l'information pouvant entraîner des conséquences indésirables, soulignent l'importance de traiter ces questions dès le début de la phase de conception et de développement des villes intelligentes.

Un certain nombre d'études ont présenté des analyses de la littérature sur les villes intelligentes. Cependant, la plupart de ces études semblent avoir omis de présenter une analyse significative des menaces inhérentes au développement des infrastructures urbaines intelligentes, de leurs conséquences sur le fonctionnement des villes et sur la préservation de l'ordre et la sécurité publique, et des droits fondamentaux des habitants.

Cette prospection vise à compléter la littérature existante en effectuant une analyse complète des nombreuses questions et des principales complexités liées à la sécurité et aux risques dans les projets de villes intelligentes. L'analyse et les résultats de cette recherche sont présentés comme offrant un cadre informatif et opportun pour une meilleure compréhension du sujet.

1 ETAT DE L'ART ET DES ENJEUX DES SMART CITIES

1.1 L'ORIGINE DE L'EXPRESSION DE LA VILLE INTELLIGENTE ET SA DEFINITION

L'incursion vers les villes intelligentes remonte aux années 1970, lorsque la ville de Los Angeles a créé le premier projet de Big Data urbain.[1] Mais la première ville intelligente fut sans doute Amsterdam avec la création d'une ville numérique virtuelle en 1994. Les choses se sont ensuite accélérées au milieu des années 2000 lorsque IBM et Cisco ont lancé des initiatives distinctes. En 2011, le premier Congrès mondial de la Smart City Expo s'est tenu à Barcelone, qui est maintenant devenu un événement annuel retraçant le développement des villes intelligentes. Le terme de ville intelligente ou Smart City, en anglais, a fait sa première apparition aux États-Unis dans un environnement commercial de deux entreprises technologiques, IBM et Cisco, pour évoquer un point de vue sur une ville parfaite grâce à l'utilisation efficiente et intégrée des technologies de l'information et de la communication (TIC) dans les villes. Puis l'ancien président américain Bill Clinton a été le premier dirigeant politique à introduire le concept de ville intelligente en 2005, affirmant que les villes sont en fait déjà intelligentes, mais qu'elles doivent désormais devenir durables.

Aujourd'hui, il n'existe aucun ensemble de termes ou de définitions normalisés et généralement acceptés permettant de définir correctement les « villes intelligentes ». L'Union internationale des télécommunications (UIT)[2] a publié un rapport technique en 2014, qui a analysé en détail plus de 100 définitions liées aux villes intelligentes.

La définition suivante est le résultat de l'analyse de l'UIT : "*Une ville intelligente et durable (VID) est une ville innovante qui utilise les technologies de l'information et de la communication (TIC) et d'autres moyens pour améliorer la qualité de vie, l'efficacité du fonctionnement et des services urbains, et la compétitivité, tout en veillant à répondre aux besoins des générations actuelles et futures en ce qui concerne les aspects économiques, sociaux et environnementaux.*"

[1] « A Cluster Analysis of Los Angeles ».
[2] L'Union internationale des télécommunications ou UIT est l'agence des Nations unies pour le développement spécialisé dans les technologies de l'information et de la communication, basée à Genève.

Pour les besoins de notre travail, nous allons utiliser cette définition. L'analyse des différentes définitions des villes intelligentes montre que ces définitions se concentrent sur différents aspects des villes intelligentes. Cependant, il existe plusieurs caractéristiques communes d'une ville intelligente, qui peuvent être résumées dans les six thèmes principaux suivants énumérés dans le schéma ci-dessous à savoir la mobilité intelligente, l'économie intelligente, la vie intelligente, la gouvernance intelligente, les personnes intelligentes et l'environnement intelligent. Mais les facteurs spécifiques associés à ces thèmes évoluent dans le temps et dépendent du contexte spécifique de chaque ville et de son stade de développement.

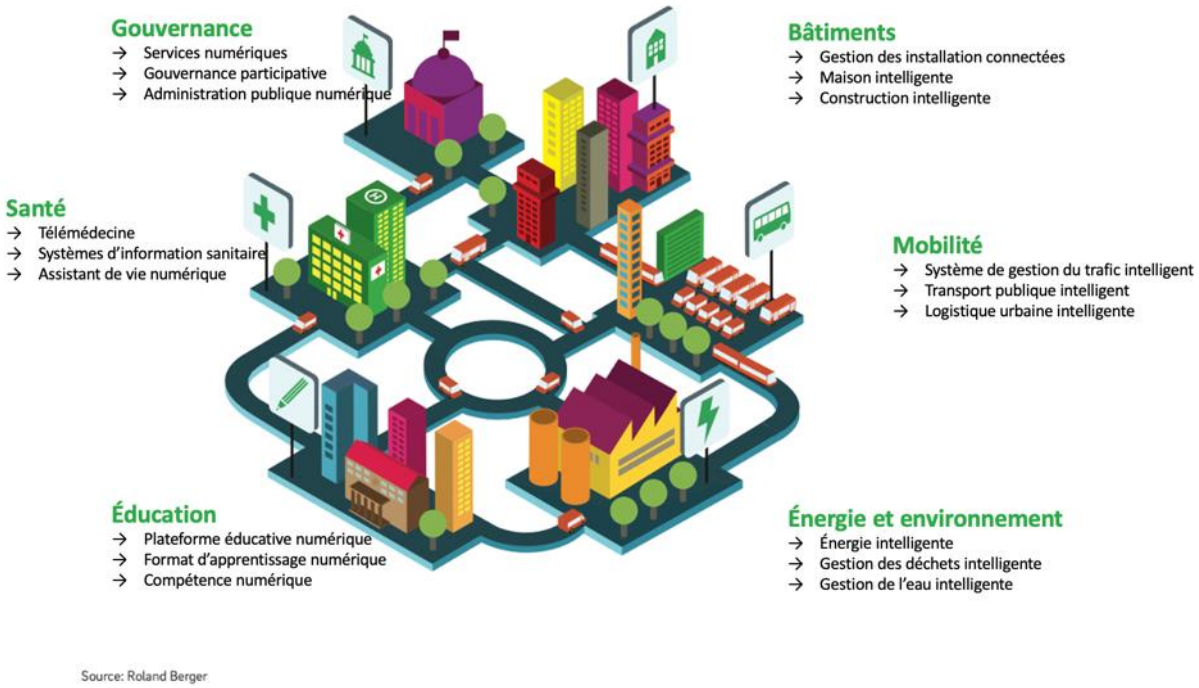


Figure 1:Les principaux thèmes de la ville intelligente (Roland Berger)

1.2 LES RAISONS D'UNE EMERGENCE RAPIDE DE LA VILLE INTELLIGENTE ET SES OBJECTIFS

L'accroissement de la population dans les zones urbaines et le maintien des principes de développement durable avec ses trois notions fondamentales : la croissance économique, le bien-être et le respect de l'environnement ont poussé à revoir le modèle de gestion développement d'une ville aujourd'hui.

En 1950, environ 65% de la population mondiale vivait dans les zones rurales, tandis que 35% vivait dans les villes. Selon [l'Organisation des Nations unies, d'ici 2050], ce nombre sera inversé, alors qu'il y aura 70% de la population urbaine et 30% de la population rurale. Ainsi, 6 milliards de personnes vivront dans les zones urbaines. La figure ci-dessous reflète la prévision de la population urbaine d'ici 2050. Toutes les régions du monde affichent une tendance à l'urbanisation, mais le taux de croissance est différent. Si l'on compare les taux de croissance projetés des populations urbaines dans diverses régions (ci-dessous), il est constaté que les pays à faible revenu sont confrontés à une croissance démographique urbaine plus rapide que les pays à revenu élevé.

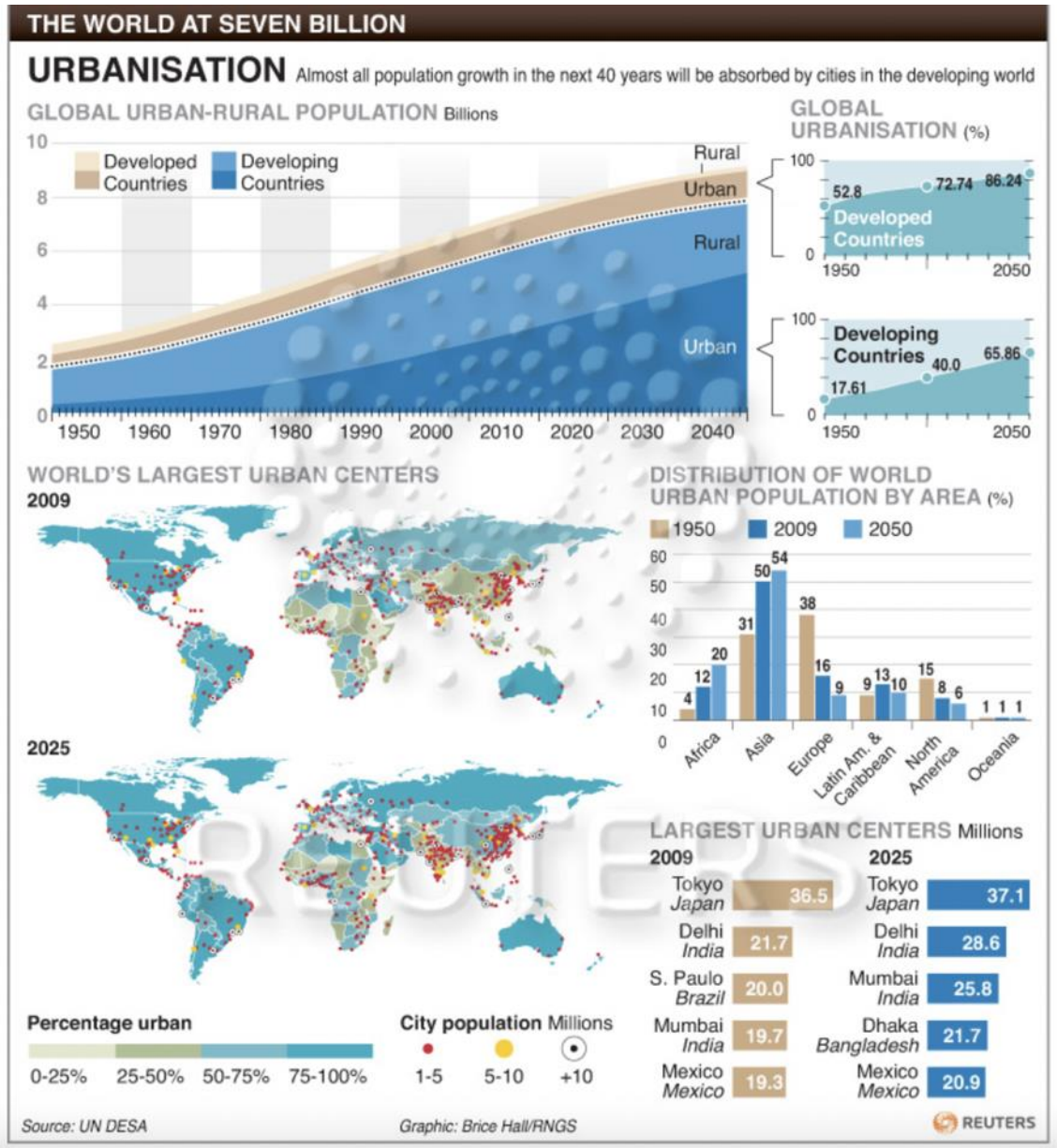


Figure 2: UN World Urbanization Prospects (UN DESA)

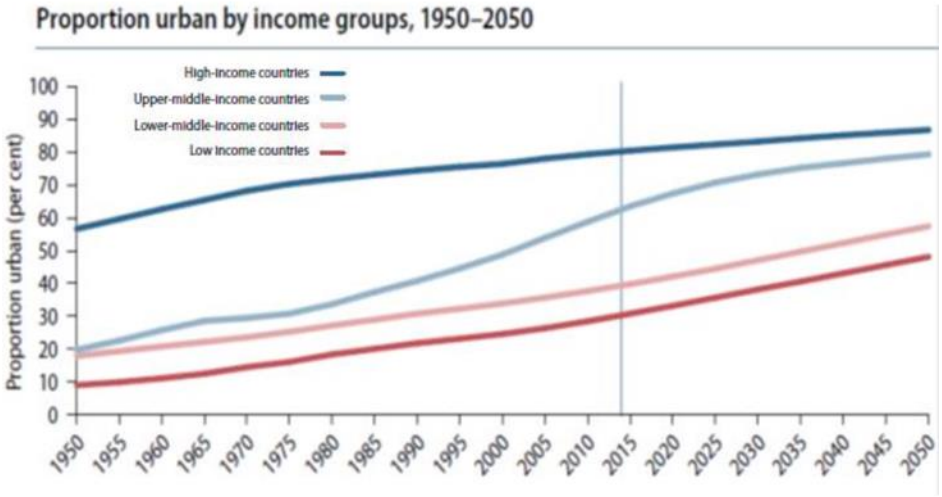


Figure 3: Urban Populations by Country Income Level - UN World Urbanization Prospects

Selon les estimations du programme des Nations unies pour l'environnement, les villes contribuent à environ 70% de la consommation mondiale d'énergie et des émissions de gaz à effet de serre, alors qu'elles n'occupent que 5 % des territoires. Cette évolution a entraîné une demande sans précédent d'eau, de terres, de matériaux de construction, de nourriture, de mesures de contrôle de la pollution et de gestion des déchets dans les zones urbaines.

Par conséquent, les villes continuent de faire face à la pression de la fourniture de services de qualité, du renforcement de la compétitivité économique locale, de l'amélioration de la prestation de services, de l'augmentation de l'efficacité et de la réduction des coûts, de l'augmentation de l'efficacité et de la productivité et de la résolution des problèmes, de la congestion et des problèmes environnementaux. Par conséquent, les villes sont constamment sous pression pour rendre des services de meilleure qualité, promouvoir la compétitivité économique locale, améliorer la prestation de services, accroître l'efficacité et réduire les coûts, augmenter l'efficacité et la productivité, s'attaquer aux problèmes de congestion et d'environnement. Ces pressions ont incité les villes à rechercher des solutions intelligentes et à essayer diverses applications d'infrastructure intelligente.

L'utilisation de technologies intelligentes dans les villes représente aujourd'hui un moyen indispensable pour réduire les émissions, surveiller la consommation d'eau, prévenir sur les niveaux de qualité de l'air, participer à la gestion intelligente des déchets, etc.

1.3 LES MODELES D'INFRASTRUCTURES DE LA SMART CITY

Les composants de l'infrastructure intelligente sont très spécifiques au contexte et leur nature est déterminée par le niveau de développement des villes ainsi que par les défis de développement spécifiques. L'infrastructure urbaine comprend en particulier le logement, l'assainissement, le traitement de l'eau et des eaux usées, l'alimentation et la distribution d'électricité, le transport, la gestion des déchets et les communications. La différence entre une infrastructure de ville intelligente et une infrastructure urbaine traditionnelle est qu'elle peut répondre et s'adapter aux changements environnementaux (y compris les besoins des utilisateurs et d'autres infrastructures) pour améliorer ses performances.

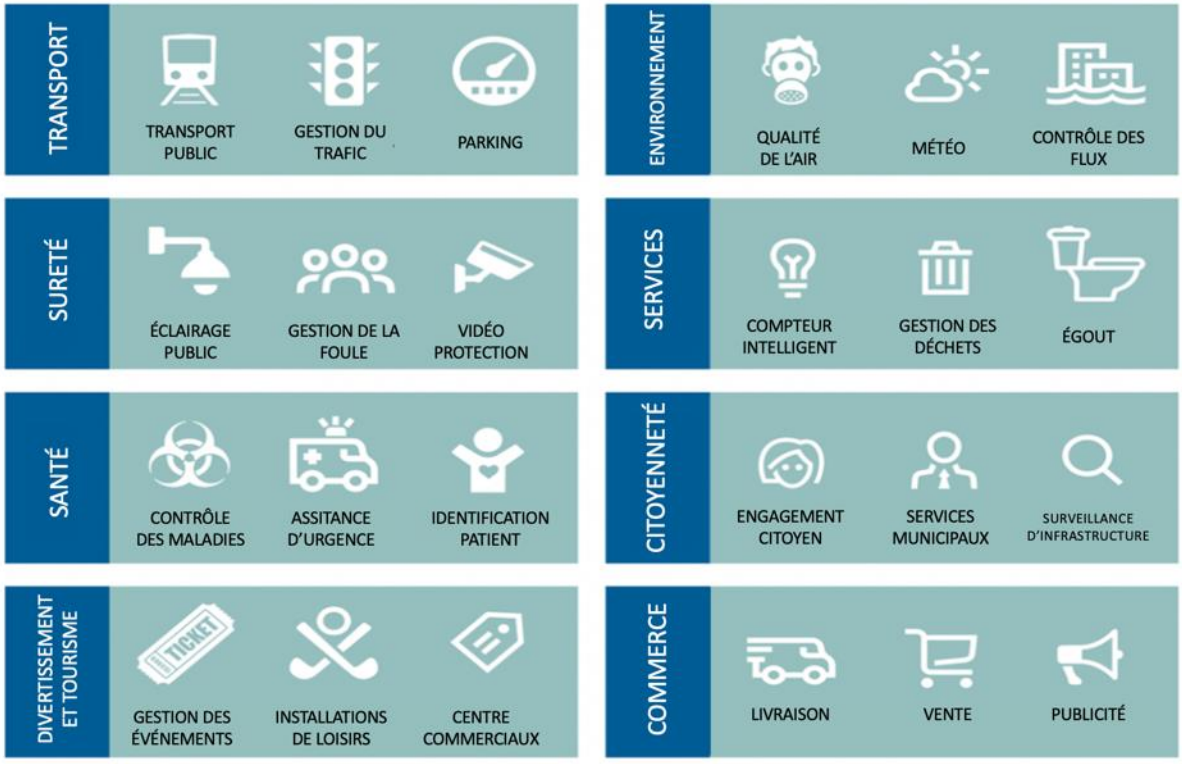


Figure 4: Diversity of IoT Applications (Carlos Bosch GSMA)

En outre, ces applications d'infrastructure ont le potentiel de fournir de nouvelles innovations qui augmenteront l'efficacité et géreront mieux les ressources. Par exemple, les données générées par la nouvelle infrastructure peuvent fournir des informations utiles pour repenser le réseau de transmission et créer de nouvelles applications mobiles destinées aux citoyens et aux services publics.

Dans les pays développés, le défi consiste à maintenir les systèmes d'infrastructure existants, qui ne peuvent être abandonnés pour des raisons évidentes de coût ou d'espace. Dans ce cas, les applications d'infrastructure intelligente se concentreraient davantage sur l'optimisation de ces infrastructures existantes et sur le contrôle de leur fonctionnement.
Par exemple, à Paris, le réseau de métro existant représente un énorme système d'infrastructure patrimoniale. Dans le cadre de sa modernisation, des trains automatisés ont été introduits sur la ligne n°1 du réseau du métro parisien, ainsi que de nouveaux systèmes audiovisuels et de contrôle de l'information. Cela a permis d'augmenter la capacité de 70 000 passagers par jour et de réduire considérablement les retards des passagers.

Cependant, dans les contextes des pays en développement comme des pays développés, la motivation première des applications d'infrastructure intelligente est qu'elles répondent aux besoins de développement durable de la société. Le tableau ci-dessous donne un aperçu de certaines solutions d'infrastructure intelligente et de la manière dont elles répondent à certains des défis de développement durable liés à l'urbanisation.

Développement durable Besoin / bénéfice	Exemple de solutions d'infrastructure intelligente	Description
Améliorer les infrastructures d'énergie et les services publics	Compteurs intelligents	Des compteurs d'électricité, d'eau et de gaz qui permettent de mesurer en temps réel la consommation d'énergie.
	Réseau électrique intelligent	Réaménagement des systèmes électriques grâce à l'utilisation de compteurs et d'appareils intelligents et de ressources énergétiques renouvelables afin d'améliorer l'efficacité énergétique.
Fournir une connectivité	Internet à haut débit	La fibre optique à domicile et d'autres solutions de connectivité émergentes,

abordable et de haute qualité		notamment le wifi public et le haut débit mobile.
Développer l'infrastructure urbaine /transport	Éclairage public intelligent à LED	Des capteurs de lumière et des dispositifs de communication pour permettre aux lumières de communiquer avec d'autres lumières proches et d'être contrôlées au niveau de la ville.
Parking/ Immeuble/ rue	Immeubles intelligents	Un ensemble de capteurs et de technologies qui améliorent la sûreté, la sécurité, l'efficacité énergétique et la convivialité.
	Véhicules électriques	Voitures fonctionnant à l'électricité avec une infrastructure appropriée pour les stations de recharge dans toute la métropole.
	Parkings intelligents	Les parkings et les emplacements de stationnement dans la rue qui transmettent des informations en temps réel aux utilisateurs.
	Feux de circulation	Détection et gestion automatisées du trafic.
Améliorer les performances environnementales	Réseau de capteurs environnementaux	Collecte continue de données sur l'état de l'air, de l'eau, du sol et des niveaux de polluants correspondants.
Assurer la sécurité et la sûreté publiques	Vidéo protection	Sécurité publique, gestion des foules et comptage des personnes à l'aide de réseaux de capteurs et de caméras en réseau.

Accroître l'efficacité de la gestion de la ville	Centre opérationnel de la ville intelligente	Suivi et gestion d'une série de services gouvernementaux, de transport, d'environnement et d'urgence
Améliorer les services de santé et d'éducation	Soins de santé à distance et enseignement en ligne	Produits et services pour l'accès à distance aux services de santé et à l'éducation.

L'infrastructure est le fondement du développement d'une ville intelligente ; elle peut être divisée en deux catégories : (1) physique et (2) numérique. Cette section fournit de brèves descriptions des infrastructures physiques intelligentes suivantes : (1) Bâtiments intelligents, (2) Mobilité et transport intelligents, (3) Énergie intelligente, (4) Gestion intelligente de l'eau, (5) Gestion intelligente des déchets et (6) Soins de santé intelligents, avec des études de cas et des exemples. En ce qui concerne l'infrastructure numérique, une brève discussion sur l'infrastructure des TIC (Technologies de l'information et de la communication) et des données est également présentée. Cette section se termine en soulignant la nécessité d'une approche intégrée pour traiter ces divers composants de l'infrastructure de la ville intelligente.

1.3.1 Infrastructures physiques

1.3.1.1 Bâtiments intelligents

Les bâtiments jouent un rôle essentiel dans une ville, car ils en sont la pierre angulaire et offrent confort et sécurité à ses habitants. Les individus ont tendance à passer plus de 80 % de leur vie à l'intérieur des bâtiments, ce qui fait que les bâtiments font partie intégrante de leur vie.

Un bâtiment intelligent intègre les différents systèmes physiques présents dans un bâtiment (tels que le système d'automatisation du bâtiment (BAS, Building Automation System) - gestion de l'énergie, système de contrôle de l'éclairage, systèmes de contrôle de la sécurité incendie et de la sécurité des personnes, systèmes de guidage et de gestion du stationnement) de manière intelligente afin de garantir que tous les différents systèmes d'un bâtiment agissent ensemble de manière optimisée et efficace.

Figure 5 : illustration d'un bâtiment intelligent (les-smartgrids.fr)

Cette intégration est généralement réalisée de manière fiable, rentable et durable, dans le but d'offrir un confort et un bien-être aux occupants et d'améliorer ainsi la productivité et les performances. Aux États-Unis, les bâtiments représentent 36% de la consommation totale d'énergie, 30 % des émissions de gaz à effet de serre, 30 % de la production de déchets (près de 136 millions de tonnes par an), 30 % des matières premières utilisées et 65% de la consommation d'électricité. Les chiffres sont similaires à l'échelle mondiale, ce qui souligne l'importance des bâtiments intelligents.

Les systèmes de gestion des bâtiments peuvent améliorer l'efficacité énergétique des bâtiments, réduire le gaspillage et garantir une utilisation optimale de l'eau tout en assurant l'efficacité opérationnelle et la satisfaction des habitants. On estime que la mise en œuvre de solutions de bâtiments intelligents pourrait permettre d'économiser jusqu'à 30 % de la consommation d'eau et 40% de la consommation d'énergie, et de réduire les coûts globaux de maintenance des bâtiments de 10 à 20 %. Il a été constaté que la consommation d'énergie dans les bâtiments existants peut être réduite jusqu'à 50% grâce à de simples programmes de modernisation.

1.3.1.2 Mobilité et transport intelligents

La mobilité et le transport intelligents sont décrits comme des approches qui réduisent la congestion et favorisent des options de transport plus rapides, plus écologiques et moins coûteuses. L'infrastructure de transport d'une ville intelligente vise à optimiser les déplacements au sein d'une ville, à économiser de l'énergie et à réduire les émissions de carbone.

La majorité des dispositifs de gestion intelligente des transports utilisent des données recueillies auprès de diverses sources afin de contribuer à optimiser les conditions de circulation de manière globale.

Selon les prévisions mondiales, publiées par « MarketsandMarkets », « *la taille du marché du transport intelligent devrait passer de 94,5 milliards USD en 2020 à 156,5 milliards USD d'ici 2025, à un taux de croissance annuel composé (TCAC) de 10,6% au cours de la période de prévision* ».

Les systèmes de mobilité et de transport intelligents peuvent être divisés dans les domaines suivants : (1) le transport de masse (2) la mobilité individuelle et (3) les systèmes de transport intelligents. Ces domaines sont examinés ci-dessous.

1.3.1.2.1 Le transport urbain de masse

La mobilité dans les villes doit s'adapter et devenir plus performante pour faire face à l'augmentation rapide de la population. Les principaux dispositifs de transport de masse pour le public sont soit le train, le métro ou les bus. Les pays développés ont depuis longtemps mis l'accent sur le transport par métro et par train à l'intérieur des frontières de la ville. Le SMRT (Singapore Mass Rapid Transit) de Singapour est un exemple de système de transport efficace dans un pays développé. Il comprend plus de 100 stations, des services de train qui circulent une fois toutes les 5 minutes et qui comptent 2,5 millions d'usagers sur une population d'environ 3,5 millions d'habitants. Le MRT est l'un des piliers du transport à Shanghai[3] et à Delhi et de nouveaux systèmes sont prévus dans de nombreuses autres villes du monde dont Jakarta qui a déjà fait l'inauguration en 24 mars 2019 de son premier tronçon de la première ligne, qui va de Lebak Bulus dans le sud au rond-point de l'hôtel « Indonésia » dans le centre.

[3] Il s'agit désormais du plus long réseau de métro du monde.

Bien que de nombreuses villes disposent de systèmes de bus, ils ne fonctionnent pas efficacement la plupart du temps. Une innovation à cet égard est le concept de Bus Rapid Transit (BRT) qui est un mode de transport public de haute qualité, efficace et basé sur le bus.

L'Institut pour les politiques de transport et de développement le définit comme suit : "*Le Bus Rapid Transit (BRT) est un système de transport en commun par bus de haute qualité qui offre des services rapides, confortables et rentables à l'échelle du métro. Pour ce faire, il dispose de voies réservées, de couloirs de bus et de stations emblématiques généralement alignées sur le centre de la route ».*

Cinq éléments essentiels placent le BRT dans le transport en commun rapide par bus :

- Des voies réservées aux bus pour éviter les embouteillages ;
- Les arrêts et les voies d'autobus alignés au centre de la rue pour éviter d'être retardés par des véhicules qui tournent et des véhicules déposant des passagers ou des marchandises ;
- La mise en place de « ticket SMS » ou via des applications dédiées aux achats des billets, pour éviter les retardements causés par les passagers payant à bord ;
- Embarquement à partir d'une plate-forme au niveau du plancher du bus pour accélérer l'embarquement et permettre aux personnes en fauteuil roulant ou en poussette d'accéder directement dans le transport ;
- Les restrictions de virage et la priorité des bus aux intersections pour réduire les délais aux intersections des feux rouges

Figure 6 : Bus Rapid Transit - BRT (itdp.org)

1.3.1.2.2 La mobilité individuelle

Traditionnellement, la mobilité "individuelle" dans les villes passe par une forme de transport motorisé, principalement la voiture ou les véhicules motorisés (moto, scooter, …). Il semble y avoir un mouvement d'abandon de la voiture au profit d'un système de transport conçu autour de la mobilité individuelle, qui comprend le vélo, le covoiturage, l'autopartage et, plus récemment, le transport à la demande.

- **Déplacements à bicyclette :**

Ces dernières années, les déplacements à vélo sont de plus en plus attrayants. Dans les villes, pour les déplacements sur de courtes distances, la bicyclette est souvent le mode de transport le plus rapide. Pékin et Shanghai, par exemple, réintroduisent actuellement des pistes cyclables pour favoriser et encourager les déplacements en vélos.

Un concept intéressant lié aux vélos est le système de vélos en libre-service avec la présence de multiples prestataires de services comme Clear Channel pour Bicing à Barcelone ou Veloway pour Vélo Bleu à Nice. Le principe est très simple : un habitant de la ville prend un vélo (moyennant une redevance) à un point de ramassage donné (A), l'utilise pour se rendre à un autre point (B) et le dépose afin qu'un autre habitant puisse ensuite le prendre du point B au point C, et ainsi de suite. Ce système est extrêmement populaire à Amsterdam, Budapest, Paris, San Francisco et Barcelone.

Par exemple, à Paris, le réseau, appelé VELIB, est composé de 1 400 stations et de plus de 20 000 vélos disponibles (dont 35% à assistance électrique). En 2020, ce réseau comprenait 400 000 abonnés avec des pics autour de 150 000-200 000 de trajets journaliers.

Figure 7 : Vélopartage Velib Parisien (wikiwand.com)

La convergence des nouvelles technologies telles que les cartes à puce, le haut débit mobile et les technologies de téléphonie intelligente permet de tirer parti du vélopartage de nombreuses manières innovantes, notamment en effectuant des réservations, en trouvant les points de prise en charge et de dépose les plus proches et les conditions de circulation couplées aux cartes des pistes cyclables d'une ville.

- **Covoiturage[4] et Autopartage[5] :**

Le covoiturage utilise les sièges vides des voitures de manière efficace, ce qui réduit l'impact négatif sur l'environnement et en fait un processus durable. On estime qu'une voiture en covoiturage remplace 5 à 8 voitures privées et libère jusqu'à 1,5 à 3 places de stationnement dans la rue. Utilisé de manière plutôt ponctuelle, il constitue désormais un bon complément à d'autres formes de mobilité durable. Cependant, le covoiturage a connu une tendance à la baisse au cours des dernières décennies. Les progrès technologiques tels que le géolocalisation et les applications mobiles jouent un rôle important pour contrer cette tendance à la baisse.

[4] Définis *"… comme l'utilisation en commun d'un véhicule terrestre à moteur par un conducteur et un ou plusieurs passagers, effectuée à titre non onéreux, excepté le partage des frais, dans le cadre d'un déplacement que le conducteur effectue pour son propre compte"* - l'article L.3132- du code des transports.

[5] Définis *"… comme étant « la mise en commun d'un véhicule (…) au profit d'utilisateurs abonnés ou habilités par l'organisme ou la personne gestionnaire des véhicules » - L'article L.1231-14 du code des Transports.*

Des applications telles que BlaBlaCar, Ubeeqo mettent en relation des conducteurs et des passagers (qui empruntent des itinéraires similaires) en temps réel, sans planification préalable, ce qui améliore l'accessibilité. Bien que le covoiturage soit plus courant dans les pays développés, il n'est pas beaucoup adopté dans les pays en développement, en grande partie à cause d'une combinaison de normes sociales, de faibles taux de possession de voitures et d'un manque d'heures de travail standardisées.

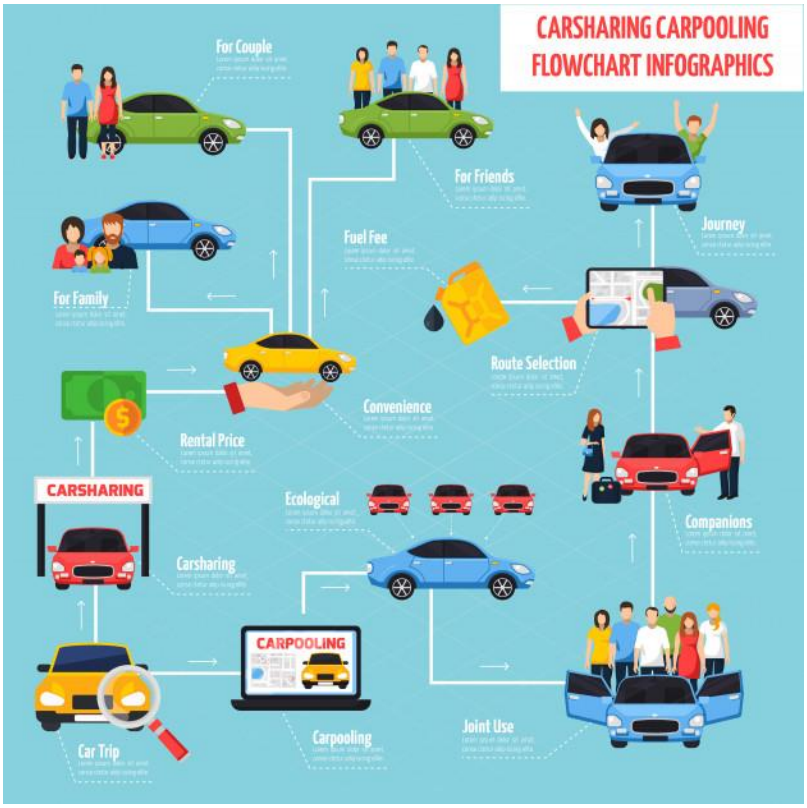


Figure 8 : l'illustration d'un autopartage et covoiturage (canstockphoto.fr)

L'autopartage est un concept légèrement différent du covoiturage dans la mesure où il permet aux gens de louer des voitures à l'heure. On peut considérer qu'il s'agit d'une location de voiture à l'heure, mais la différence est similaire à celle du vélopartage : il existe plusieurs points de prise en charge et de dépose pour les utilisateurs, ce qui réduit l'espace de stationnement en ville, où à la place de plusieurs voitures, une seule voiture peut faire le travail. Les utilisateurs paient une cotisation annuelle ou des frais de location à l'unité et peuvent réserver des voitures, y compris l'essence, l'entretien, l'assurance et le stationnement. Donc on peut distinguer 3 types de l'autopartage :

- L'autopartage entre particuliers : famille, proches, amis, voisins, etc.

- La location des véhicules entre les particuliers : grâce aux sites d'internet ou d'applications spécialisées pour smartphones dédiés.
- Les services d'autopartage : s'effectuent généralement au sein des villes, via des parcs de voitures en libre-service.

1.3.1.2.3 Les systèmes de transport intelligents

Les systèmes de transport intelligents (STI) intègrent de manière efficace l'ensemble des options de transport multimodal d'une ville, y compris les options de mobilité individuelle et de transport en commun. Les derniers STI comprennent, entre autres, un réseau de capteurs, des voitures connectées, des transports publics avec suivi GPS, des feux de circulation dynamiques, des panneaux d'information pour les passagers, des lecteurs automatiques de plaques d'immatriculation, des systèmes de télévision en circuit fermé, des installations de navigation, des systèmes de signalisation et, surtout, la capacité d'intégrer des données en direct provenant de la plupart de ces sources. Cela peut conduire à des améliorations majeures en matière de sécurité, de gestion du réseau, de congestion du trafic, de performance environnementale, d'accessibilité, de commodité et de perception du public.

En 2017, la ville d'Ahmedabad a lancé un projet de système de transport intelligent combinant 3 initiatives à savoir l'Integrated Transit Management System (ITMS), Automated Fare Collection System (AFCS) et Common Card Payment System (CCPS) ; ce système a ainsi permis de réduire les temps d'attente des transports publics, surveiller en temps réel le trafic et l'utilisation d'un mode de paiement unique incluant les transports informels.

Depuis 1998, Singapour a introduit le système de Tarification électronique des routes (Electronic Road Pricing, ERP) pour gérer les embouteillages. Malgré la forte croissance démographique, l'ERP a réduit le trafic dans le centre-ville de 24% et en moyenne les vitesses sont passées de 30 à 35 km/h à 40-45 km/h. Cependant, la ville se concentre également sur l'utilisation de véhicules connectés, avec des plans de lancement de bus automatisés dès 2022. La ville a été nommée au top de classement par KPMG (un cabinet de conseil en stratégie) dans la mise en place du système des véhicules automatisés

1.3.1.3 Réseau électrique intelligent

L'augmentation des prix de l'énergie, l'épuisement des sources et le réchauffement de la planète dû à l'impact de l'utilisation de l'énergie sont quelques-uns des problèmes clés que

les collectivités cherchent à résoudre dans leur cheminement vers le développement durable. Les systèmes de gestion intelligente de l'énergie constituent une solution potentielle aux problèmes susmentionnés. Ils utilisent des capteurs, des compteurs avancés, des sources d'énergie renouvelable, des commandes numériques et des outils d'analyse pour automatiser, surveiller et optimiser la distribution et l'utilisation de l'énergie. Ces systèmes optimisent le fonctionnement et l'utilisation du réseau en équilibrant les besoins des différents acteurs concernés - consommateurs, producteurs et fournisseurs.

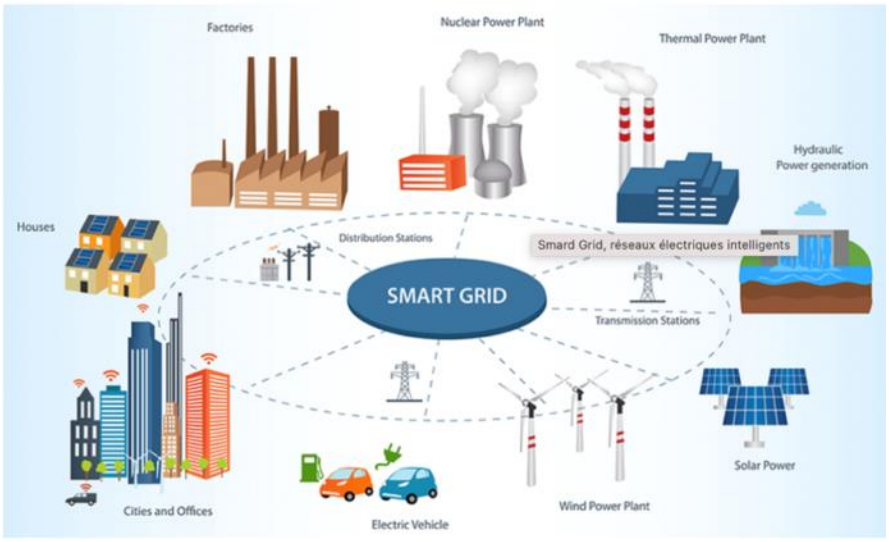


Figure 9 : illustration « réseau électrique intelligent » du site xpair.com

Le terme « *Énergie intelligente* » consiste à répondre aux besoins en énergie d'une manière écologiquement durable en utilisant un effort rentable à long terme. Il existe un certain nombre d'innovations dans l'infrastructure énergétique intelligente, telles que : la production renouvelable distribuée[6], les micro-réseaux[7], les nouvelles technologies de réseau intelligent avec l'intégration les nouvelles technologies de l'information et de la communication (NTIC) pour développer une multitude de nouveaux usages, le stockage d'énergie[8], la réponse automatisée à la demande, les centrales électriques virtuelles[9], et les innovations du côté de

[6] Les sources de production distribuée ou décentralisé comprennent : les énergies renouvelables telles que l'énergie éolienne et solaire ; la valorisation énergétique des déchets ; et la production combinée de chaleur et d'électricité (CHP, Combined Heat and Power ; également appelée cogénération), qui consiste à récupérer la chaleur produite par une centrale électrique conventionnelle pour chauffer des bâtiments et / ou de l'eau.

[7] « *Un micro-réseau est un réseau de distribution d'électricité composé d'une génération, d'un stockage et d'une charge multiples, gérés à partir du réseau de transport plus étendu* ».

[8] « *Consiste à mettre en réserve une quantité d'énergie provenant d'une source en un lieu donné, sous une forme aisément utilisable, pour une utilisation ultérieure* ».

[9] « *Une centrale électrique virtuelle est une combinaison d'unités décentralisées du réseau électrique coordonnées moyennant un système de régulation commun* ».

la demande comme les véhicules électriques et les appareils intelligents. Ces éléments de la nouvelle infrastructure énergétique fournissent un réseau étendu d'appareils énergétiques intelligents présents dans toute une ville, ce qui permet d'obtenir une vue détaillée des schémas de consommation d'énergie, de mettre en place des programmes de surveillance énergétique communautaires et d'améliorer l'efficacité énergétique des bâtiments. Désormais, à la couche physique pour le transit d'énergie des réseaux vient se superposer une couche numérique grâce aux nombreux points d'interface (capteurs, automates, etc.) pour relier ces deux couches. Les compteurs évolués de type Linky pour l'électricité et Gazpar pour le gaz naturel sont des éléments essentiels de cette nouvelle architecture des réseaux en France.

Le ministère américain de l'énergie définit un réseau intelligent comme suit *:"Un système de livraison d'électricité (du point de production au point de consommation) intégré aux technologies de communication et d'information pour améliorer les opérations du réseau, les services aux clients et les avantages environnementaux."*

Les réseaux intelligents sont mis en œuvre dans le monde entier, tant dans les pays développés que dans les pays en développement, comme illustré ci-dessous. Cela souligne la valeur et l'importance de la nécessité d'un réseau intelligent.

Pays	Projet	Description
Amsterdam, Pays-Bas	Amsterdam Ville Intelligence	De nombreux projets liés à l'énergie et au réseau intelligent ont été développés, notamment les réseaux de distribution intelligents, les maisons intelligentes, la gestion des déchets, les programmes d'efficacité des bâtiments et la gestion de la demande.
France, Auvergne-Rhône-Alpes	Projet CORRI-DOOR	« Il a pour but de déployer, en France, un réseau de 200 bornes pilotes de recharge rapide, afin de faciliter les

Provence-Alpes-Côte d'Azur		parcours en véhicules électriques sur de grandes distances. Ce déploiement devrait favoriser le développement du véhicule électrique en France en rassurant le consommateur de pouvoir se recharger n'importe où ».
France, Nice	Projet Nice Grid	« Le projet a testé un quartier solaire intelligent intégrant une part importante de production photovoltaïque locale, des solutions de stockage d'électricité, 2 500 compteurs évolués Linky et des solutions d'effacement et notamment de modulation de la consommation (déplacement des consommations électriques des clients), pour améliorer la gestion des pointes de consommation et/ou de production électriques à différentes échelles de temps ».
Australie	Projet SHIELD	Ce projet vise à développer un logiciel qui agrège des données provenant de diverses sources pour aider les fournisseurs de services de réseau de distribution à gérer les ressources énergétiques distribuées dans les réseaux basse tension.
Europe, Asie-Pacifique (Allemagne, Autriche, Hongrie et Inde)	Projet IElectrix	Il va permettre d'accélérer l'intégration des énergies renouvelables aux réseaux de distribution et de contribuer à la décarbonation du système énergétique.

Chine, Qingdao	Projet 5G Smart grid	Le réseau intelligent 5G peut non seulement supprimer automatiquement les défauts des lignes de distribution en quelques millisecondes, mais également réduire la consommation d'énergie de chaque station de base[10] 5G de 20%. Cela atténue considérablement le problème de la consommation d'énergie élevée.

Leurs avantages sont nombreux, mais certains des aspects les plus marquants sont les suivants : réduction des coûts, augmentation de l'efficacité du système et environnement plus propre. Parmi les avantages spécifiques, on peut citer la réduction des coûts d'exploitation, l'augmentation des revenus grâce à la réduction des vols d'énergie, l'amélioration de la trésorerie grâce à une gestion plus efficace de la facturation et des revenus, la réduction des pertes de transmission et de distribution, l'augmentation de la satisfaction des clients, la réduction des pics de charge et de consommation d'énergie, l'amélioration des prévisions de charge, l'augmentation de la capacité d'intégration des ressources renouvelables, la réduction des émissions de carbone grâce à une exploitation efficace, la réduction des pertes du système et l'augmentation générale des économies d'énergie…

[10] « Dans un système de radiocommunication mobile terrestre, une station de base est un équipement installé sur un site et muni d'une antenne émettrice-réceptrice avec lequel communiquent les appareils mobiles, pour avoir accès à un réseau de télécommunications » source.

1.3.1.4 Infrastructure d'eau intelligente

En 2020, plus de 700 millions de personnes dans le monde n'ont pas eu accès à l'eau potable, dont plus de 60 % en Afrique subsaharienne et en Asie du Sud ; 2,5 milliards de personnes n'ont pas eu accès à des installations sanitaires adéquates ; et le taux de mortalité annuel est de 6 à 8 millions de personnes en raison de catastrophes et de maladies liées à l'eau. L'impact des maladies liées à l'eau est plus important que l'impact combiné du VIH, de la tuberculose et du paludisme. Si l'on ajoute à ce problème celui de l'urbanisation et du manque d'assainissement, on obtient un défi et un problème majeur pour les villes. Les villes tentent donc constamment de résoudre ces problèmes grâce à des technologies innovantes et à une meilleure gestion de l'eau et de l'énergie. L'amélioration du comptage et de la gestion des flux est la clé d'un bon système de distribution d'eau. Dans les pays en développement, où les bidonvilles abritent d'immenses habitats informels et où l'accès à l'eau potable est limité, le principal problème est de mesurer la consommation d'eau, de détecter les fuites dans les réseaux de canalisations vieillissants et d'assurer un bon assainissement.

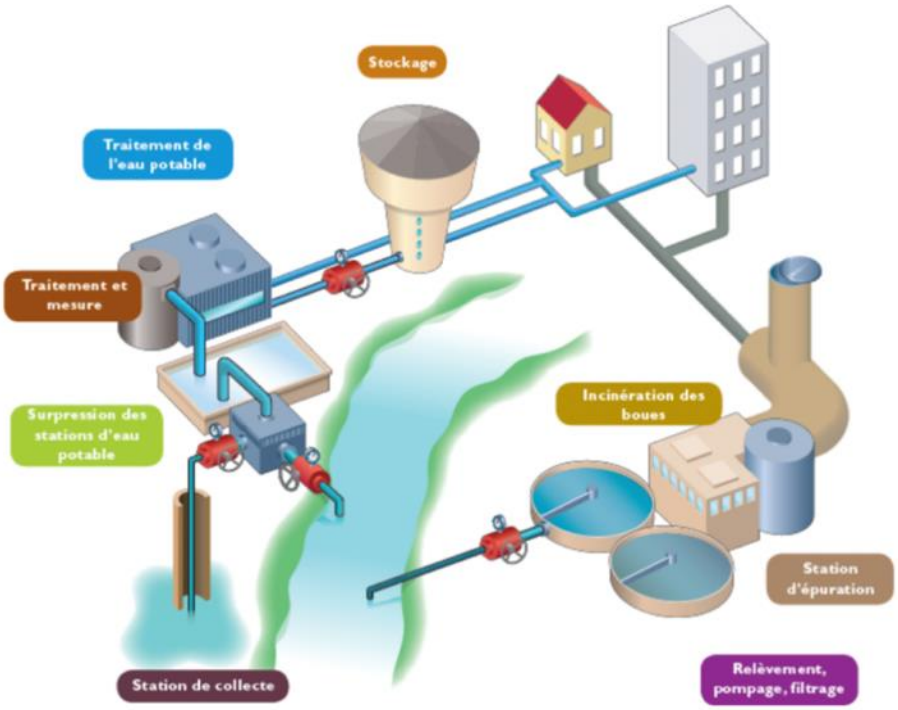


Figure 10 illustration de la chaine de distribution et de traitement des eaux - Vinci

Un système de gestion intelligente de l'eau utilise les technologies de l'information et de la communication (TIC) afin d'économiser l'eau, réduire les coûts et augmenter la fiabilité et la

transparence de la distribution de l'eau. Il y a une superposition d'un réseau de données avec le réseau physique de canalisations. Le système analyse généralement les données de débit et de pression disponibles pour déterminer les anomalies (telles que les fuites) en temps réel afin de mieux gérer les flux d'eau.

Un réseau d'eau intelligent entièrement intégré permet ce qui suit :

- La surveillance continue des réseaux de distribution d'eau et le diagnostic à distance des problèmes.
- Le contrôle des réseaux de distribution d'eau et l'optimisation en se basant sur les données.
- La fourniture d'informations aux consommateurs et de services pour qu'ils puissent suivre leur consommation.
- Le respecte des exigences de la politique de l'eau[11] et de transparence vis-à-vis des autorités de régulation.

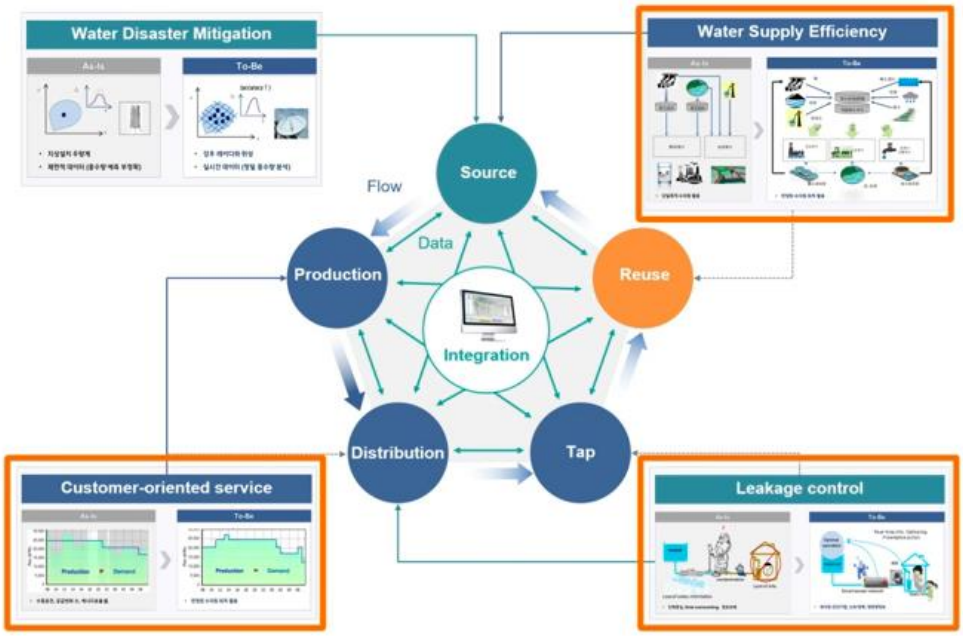


Figure 11 Le concept de la gestion réseau d'eau intelligent [K-Water Research Institute, Corée du Sud]

Ainsi, un dispositif de gestion de l'eau permet de réduire les coûts de maintenance, d'économiser l'eau, d'améliorer la sécurité de l'eau, de réduire les fuites, d'améliorer les paramètres de qualité de l'eau et de fournir une meilleure visibilité du réseau de distribution d'eau à la compagnie des eaux. Les clients finaux peuvent recevoir des informations en temps réel de la situation de leur consommation, ce qui entraîne une baisse des factures.

[11] « *Fondée sur quatre grandes lois et encadrée par la directive-cadre européenne sur l'eau publiée en 2000* »:

Pays	Projets	Description
Royaume Unis, Londres	Projet SmartH2O	Afin de démontrer comment la conscience sociale et les instruments de tarification dynamiques peuvent modifier le comportement de l'utilisation de l'eau (Projet SmartH2O), l'entreprise Thames Water a installé environ 4000 compteurs intelligents pour recueillir des relevés fréquents de compteurs (intervalles de 15 min).
Singapore	Projet compteur d'eau intelligent	Après énième projet Smart Water grid réalisé ces dernières décennies, un autre projet se prépare – installation de 3 millions compteurs d'eau intelligents sur deux ans.
Italie, Espagne et Brasil	Projet SWAMP, Plateforme de gestion intelligente de l'eau	Développement des méthodes et des approches basées sur l'IoT pour une gestion intelligente de l'eau dans le domaine de l'irrigation de précision.
Australie, llawarra-Shoalhaven	Projet llawarra-Shoalhaven	Utilise des solutions technologiques intelligentes, analyses de données pour répondre et améliorer la gestion des eaux pluviales, la qualité de l'eau, l'atténuation des inondations et l'accès à l'information pour assurer la sécurité de la population lors des crues soudaines.
États de Negeri Sembilan et de Penang, en Malaisie	Projets d'usine de traitement des eaux	« L'usine est conçue pour collecter l'ensemble des données relatives au débit, à la pression et à la distribution de

		l'eau dans les communes environnantes. Son objectif premier est de veiller à l'efficacité de la gestion de l'infrastructure et de l'énergie consommée pour distribuer l'eau ».
Japon	Projet système LED UV	Ce projet vise à prouver l'applicabilité d'une technologie hautement innovante et durable (système LED UV) pour un traitement de l'eau sans produits chimiques

1.3.1.5 Gestion intelligente des déchets

Selon une étude de la Banque mondiale[12], la production de déchets augmente à un rythme plus rapide que celui de l'urbanisation. Les villes éprouvent des difficultés à trouver, trier et utiliser différents types de déchets qui peuvent potentiellement être réintroduits dans le cycle de vie des consommateurs. On estime qu'environ 3 milliards de résidents urbains ont généré plus de 1,4 milliard de tonnes de déchets pour la seule année 2012. Ce chiffre devrait presque doubler pour atteindre 2,4 milliards de tonnes en 2025, pour une population urbaine de 4,3 milliards de personnes.

Une gestion efficace des déchets contribue à améliorer la qualité de vie des citadins, car elle permet non seulement d'améliorer la vie environnementale et de réduire les risques sanitaires, mais peut également avoir un impact économique positif sur la ville grâce au recyclage, à la réutilisation et à l'élimination. La gestion des déchets comprend généralement la surveillance, la collecte, le transport, le traitement, le recyclage et l'élimination.

[12] What a Waste: A Global Review of Solid Waste Management, World Bank, 2012.

Figure 12 : Solution de collecte intelligente des déchets (Ecube Labs)

Les systèmes de gestion des déchets sont conçus pour relever certains de ces défis. Ils réduisent le gaspillage à la source, catégorisent le type de déchets à la source et développent des méthodes pour une utilisation appropriée des déchets. Les systèmes de gestion des déchets peuvent être utilisés pour convertir les déchets en ressources et créer des économies en circuit fermé.

L'une des principales inefficacités de la gestion des déchets est l'incapacité à prévoir quand les déchets doivent être ramassés. Souvent, des camions sont envoyés pour collecter les déchets alors que les poubelles ne sont pas pleines, ce qui signifie que moins de tournées de camions sont nécessaires ou à des fréquences plus faibles, tandis qu'à d'autres moments, les poubelles débordent, ce qui nécessite plus de tournées de camions à une fréquence plus élevée. Plus de passages de camions signifient plus de temps et de carburant, et donc plus de coûts. Les capteurs, la connectivité et l'Internet des objets (IoT) offrent des moyens d'atténuer ces coûts supplémentaires.

Les principaux avantages de la gestion intelligente des déchets résident dans l'amélioration de l'efficacité de la collecte, du ramassage, du tri, de la réutilisation et du recyclage des déchets. L'élimination des déchets peut être contrôlée pour s'assurer qu'elle est effectuée de manière écologique, les flux de déchets peuvent être évalués et les solutions de recyclage et d'élimination appropriées mises en œuvre. La collecte des déchets peut être rationalisée dans toute la ville, ce qui permet de réduire les déplacements des camions. L'efficacité et les

performances globales de la collecte des déchets peuvent être contrôlées en permanence. L'optimisation du transport des déchets entre les points de collecte et les sites d'élimination ou de recyclage permettent de réduire les émissions de carbone et les charges de transport dans les rues et sur les routes de la ville.

En 2014, à Séoul, les autorités ont installé des poubelles innovantes qui compactent leur contenu avec un compresseur solaire et dotées de capteurs permettant d'organiser la collecte des déchets et de multiplier par quatre la capacité de stockage. Aussi, des capteurs ont été installés sur les bacs traditionnels afin de capitaliser les acquis et réduire les coûts.

1.3.1.6 Soins de santé intelligents

La gestion intelligente des soins de santé convertit les données relatives à la santé en informations cliniques et commerciales, ce qui inclut les diagnostics à distance, les traitements à distance, les dossiers médicaux numériques, les services de santé à domicile et les systèmes de surveillance à distance des patients.

Ainsi, l'expression "soins de santé intelligents" désigne la fourniture de soins de santé à l'aide de technologies intelligentes et en réseau qui permettent de surveiller l'état de santé des citoyens. Ils permettent de mettre l'accent sur la prévention plutôt que sur la guérison, avec une vision plus large des soins globaux, de la vie saine et de la gestion du bien-être. Elle s'applique à la fois aux environnements des patients internes et externes, garantissant la disponibilité des soins de santé et des ressources appropriées au bon moment. Les systèmes de santé intelligents sont utilisés dans les pays développés et en développement. Voici quelques exemples de soins de santé intelligents :

- La collecte à distance des données vitales du patient à des fins de diagnostic.
- L'utilisation de plateformes mobiles pour afficher les signaux électriques produits par le cœur qui sont mesurés par un capteur connecté au mobile.
- La conversion du smartphone en un appareil spécifique au patient qui mesure, affiche et communique les données générées par les capteurs.
- L'utilisation de capteurs pour déterminer les "niveaux de glucose dans le sang", qui peuvent ensuite être visualisés sur le mobile.
- Alertes automatisées aux patients pour la prise de médicaments et les bilans de santé.
- La mise en place de notifications, d'alertes et de flux de travail pour des mesures proactives.

Figure 13 : Les objectifs de soins de santé intelligents

Les soins de santé intelligents présentent de nombreux avantages tant pour les prestataires de soins, les services hospitaliers que pour les patients finaux. Les organismes de santé et les gouvernements peuvent améliorer la santé générale de la population, mais aussi augmenter le nombre de personnes bénéficiant de soins de santé. La portée est plus large. Les patients qui n'ont peut-être jamais eu accès à un médecin ou à des diagnostics médicaux pourront désormais s'engager auprès du corps médical pour améliorer leur bien-être et leur santé. Les soins préventifs sont plus viables, ce qui réduit les coûts globaux, car les coûts ultérieurs de traitement d'une maladie sont beaucoup plus élevés que les coûts de prévention.

1.3.1.7 Sécurité publique

Il existe un large éventail de technologies qui peuvent contribuer à améliorer la sécurité et l'ordre public. Nombre d'entre elles concernent le suivi et la prédiction des crimes, aidant les autorités à dissuader et à prévenir les activités illégales, ainsi qu'à faciliter les enquêtes. Voici quelques-unes des plus importantes :

- Les logiciels de police prédictive fournissent des analyses prédictives, graphiques et géographiques, de semis de points composés des faits de délinquance, incidents.
- La technologie de reconnaissance faciale, par exemple, la société américaine BriefCam développe un logiciel de reconnaissance faciale qui identifie les personnes recherche à l'aide d'images numériques extraites de vidéos ou de sources externes.

- L’éclairage public intelligent, les lampadaires équipés de capteurs environnementaux qui détectent les dangers tels que la montée des eaux, les vents violents, les températures élevées et les gaz mortels .
- Les caméras de vidéosurveillance ; les caméras de surveillance routière, le système de contrôle vidéo pour la détection des infractions et des incidents.
- Les lecteurs de plaques d'immatriculation automatisés.
- Les systèmes de détection de détonation d’armes à feu.
- Les caméras piéton de la police.

La technologie des villes intelligentes a un potentiel énorme dans le domaine de la sécurité publique, mais nombre de ces applications sont également parmi les plus controversées. En effet, bon nombre des approches de la ville intelligente mentionnées précédemment n'ont pas besoin de collecter des informations permettant d'identifier les individus pour fonctionner.

Vous pouvez recueillir des données sur le nombre de personnes utilisant un système de transport, ainsi que sur le moment et l'endroit où il est utilisé, sans avoir à savoir qui l'utilise exactement. En revanche, lorsqu'il s'agit de prévention et d'investigation de la criminalité, les autorités veulent généralement connaître l'identité des personnes impliquées pour faciliter les enquêtes et les arrestations.

Si les systèmes de détection de la criminalité sont déployés dans toute une ville, ils pourraient faire disparaître l'anonymat de la vie urbaine, ce qui pourrait avoir des coûts sociaux importants.

1.3.2 Infrastructure numérique intelligente

La ville intelligente fait un usage efficient de toutes les informations interconnectées disponibles pour mieux comprendre et contrôler ses opérations et optimiser l'utilisation de ressources limitées. Les TIC jouent un rôle important dans ce processus, car elles permettent de créer une plateforme numérique à partir de laquelle un réseau d'informations et de connaissances peut être créé. Une telle plateforme facilite non seulement l'agrégation des informations sur la ville pour l'analyse des données, mais elle peut également être utilisée pour mieux comprendre et optimiser le fonctionnement de la ville.

Les municipalités et les parties prenantes peuvent utiliser ces informations pour créer de nouvelles politiques et réglementations afin d'améliorer la qualité de vie des citoyens.

L'une des principales propositions de valeur des TIC dans une ville intelligente est la capacité de saisir et de partager les informations en temps utile. Même si une ville est bien équipée pour répondre à une situation donnée, si les informations ne sont pas fournies et partagées rapidement, les problèmes spécifiques, tels que les embouteillages ou les pannes de services publics, risquent de ne pas être résolus rapidement. Si les informations sont fournies en temps réel et avec précision, les villes peuvent potentiellement prendre des mesures avant que le problème ne commence à s'aggraver. Une ville peut donc être considérée comme une "ville prédictive", où des événements et des incidents spécifiques peuvent être prévus, ce qui améliore la qualité de vie et permet aux citoyens d'être mieux informés de la situation, afin qu'ils puissent prendre une décision éclairée quant à la prochaine action à entreprendre.
Une façon d'appréhender l'infrastructure numérique est de la considérer sous la forme de différentes couches de support numérique, comme décrit ci-dessous.

1.3.2.1 Couche urbaine

C'est là que les infrastructures physiques et numériques se rencontrent. En voici quelques exemples : Bâtiments intelligents, réseau intelligent (services publics - eau, électricité, gaz), gestion de déchets intelligente et mobilité intelligente.

1.3.2.2 Couche capteurs

Les dispositifs intelligents qui mesurent et surveillent différents paramètres entrent dans cette catégorie. L'objectif est de pouvoir détecter de multiples paramètres tels que l'humidité, l'eau, l'énergie, la qualité de l'air, la température, le flux solaire, l'occupation et l'état des équipements.

1.3.2.3 Couche de connectivité

Cette couche traite de la capacité à transporter les données et les informations depuis le capteur vers les agrégateurs de données et le stockage pour une analyse ultérieure. Une ville intelligente disposera d'une gamme complète de réseaux maillés de capteurs à faible bande passante, de réseaux étendus à large bande passante et de tout ce qui se trouve entre les deux.
La mise en œuvre des technologies des villes intelligentes nécessite souvent un réseau à large bande robuste, fiable et abordable. Cela souligne la nécessité de continuer à se concentrer sur la réduction de la fracture numérique, afin d'exploiter les avantages des applications

intelligentes. Le haut débit mobile joue également un rôle majeur, en particulier dans les pays en développement, où l'infrastructure fixe fait défaut. La révolution des téléphones intelligents avec les "applications" a déjà pris racine et il existe de nombreuses applications liées aux villes intelligentes, notamment en matière de circulation, de santé, d'énergie et d'eau.

1.3.2.4 Couche d'analyse des données

Les solutions d'analyse des données sont de trois types principaux : (1) Descriptive, qui utilise la veille économique et l'exploration de données pour demander : "Que s'est-il passé ?". (2) Prédictive, qui utilise des modèles statistiques et des prévisions pour demander : "Que pourrait-il se passer ?" et (3) Prescriptive (y compris Cognitive), qui utilise l'optimisation et la simulation pour demander : "Que devrions-nous faire ?".

1.3.2.5 Couche d'automatisation

Il s'agit de la couche d'interface numérique qui permet l'automatisation et l'évolutivité d'un grand nombre de dispositifs dans plusieurs domaines. Elle permet à la ville ainsi qu'à ses partenaires de l'écosystème de développer des services et des initiatives intelligentes.

1.3.2.6 Couche Internet des objets

L'Internet des objets (IoT) tel que défini par Ashton est « *l'endroit où tous les objets et équipements de ce monde seront connectés par Internet. Et les données générées par tous ces objets permettront aux ordinateurs de savoir beaucoup de choses sur les gens*". L'IoT peut être considéré comme une infrastructure mondiale qui relie les dispositifs TIC dans le monde entier. L'IoT ne consiste pas seulement à connecter les humains avec les objets, mais les objets peuvent également interagir entre eux, par exemple une fuite dans un tuyau peut être communiquée au compteur d'eau. Dans une étude du MIT, les chercheurs ont pu suivre près de 3 000 déchets à l'aide d'étiquettes intelligentes et ont découvert que certains de ces déchets voyagent depuis leur lieu d'origine aux États-Unis pendant plus de trois mois avant d'atteindre une unité d'élimination des déchets. Sur la base de ces découvertes, l'efficacité des systèmes dans une ville peut être améliorée.

1.4 LA NECESSITE D'UNE APPROCHE INTEGREE POUR LES INFRASTRUCTURES INTELLIGENTES

Une ville a de nombreuses fonctions physiques qui se manifestent dans les différentes formes d'infrastructures - eau, déchets, bâtiments, etc. Chaque élément d'infrastructure est un système et se compose de sous-systèmes, de composants et de dispositifs qui se comportent comme un réseau de données en communiquant entre eux. La ville est constituée de ces différentes infrastructures verticales formant un « système multicouche ». Il existe un lien évident entre ces différents systèmes. Par exemple, un bâtiment consomme de l'énergie, de l'eau et génère des déchets ; si les différents systèmes intelligents individuels sont réunis, le bâtiment devient "intelligent". Cependant, dans de nombreux cas, ces éléments d'infrastructure urbaine ont tendance à fonctionner en silos. Les villes intelligentes nécessitent un traitement intégré de toutes les infrastructures intelligentes. Des moyens plus intelligents de développer les villes apparaîtront lorsque les administrations municipales et les citoyens commenceront à penser et à planifier les éléments d'infrastructure de manière holistique.

Les TIC peuvent faciliter ce processus. Une approche couramment utilisée consiste à regrouper les différents flux de données de la ville sous un système de collecte et de traitement centralisé. Cela permet la collecte et l'intégration de données provenant de différents systèmes intelligents à travers les fonctions - créant ainsi des efficacités à l'échelle du système et permettant de nouvelles perspectives. Ces centres d'opérations font office de "centre nerveux" pour les différentes initiatives intelligentes en fournissant la base technologique nécessaire à une vision intégrée.

Les infrastructures doivent être considérées comme un système qui intègre les principaux domaines de la durabilité (à savoir, le social, l'économique et l'environnemental) dans le contexte urbain. Par exemple, en se concentrant sur les nouveaux systèmes d'énergie renouvelable de pointe par le biais d'une infrastructure énergétique intelligente, les villes sont en mesure de produire une énergie propre, de garantir la rentabilité et de réaliser simultanément un saut technologique.

1.5 LES ENJEUX LIES AU MODELE DE LA SMART CITY

1.5.1 Enjeux de souveraineté

Par son fonctionnement connecté, la ville intelligente va collecter des données pour répondre aux besoins des territoires et offrir des services aux usagers. L'informatique en nuage (cloud) est une réponse séduisante offrant une puissance de calcul et une souplesse permettant d'obtenir des résultats significatifs rapidement. Les acteurs majeurs des solutions cloud sont aujourd'hui essentiellement des grands groupes pour la plupart internationaux s répondant à des objectifs et des contraintes parfois éloignés du territoire d'utilisation.

La nature des données collectées (personnelles, santé, statistique d'usage) doit respecter strictement les contraintes réglementaires imposées par le régulateur. Il est également essentiel de ne pas négliger les aspects éthiques et communications liés à l'adoption de telle ou telle solution. Nous pouvons ici citer l'exemple de Toronto qui a dû abandonner son projet de ville intelligente basée sur une solution exclusivement Google. En effet les habitants se sont rapidement opposés à l'usage de leurs données issues de systèmes de capture vidéo par la filiale de Google.

Ainsi le cas de la création d'une Plateforme des données de santé (PDS) en France hébergée par Microsoft, également appelée « Health Data Hub » (HDH), crée par arrêté du 29 novembre 2019 comme objectif de faciliter le partage des données de santé issues de sources très variées afin de favoriser la recherche qui est aujourd'hui devenue un enjeu majeur de la protection des données de français qui ne peuvent pas être utilisées sans leurs consentements, ce qui ne sera clairement pas le cas avec Microsoft ou la décision dépendra de la législation américaine par application de Cloud Act[13] et le Patriot Act[14] . C'est une contradiction majeure du gouvernement français qui professe de la souveraineté numérique et déclare vouloir mettre fin à la domination des GAFAM (Google Amazon, Facebook et Microsoft), et en même temps impose l'utilisation du Cloud Microsoft dans la construction du HDH. Au moment même où nous finissions la rédaction de notre mémoire, l'État français présentait son nouveau plan pour s'affranchir progressivement des grands acteurs du cloud. Une nouvelle stratégie nationale pour l'hébergement des données dans un cloud souverain

[13] « Le CLOUD Act (Clarifyng Lawful Overseas Use of Data Act) est une loi américaine du 23 mars 2018 qui vise à permettre aux autorités judiciaires l'accès aux données électroniques hébergé à l'étranger ».

[14] « Le PATRIOT Act permet aux agences gouvernementales américaines (le FBI, la CIA, la NSA, l'armée) d'obtenir des informations dans le cadre d'une enquête relative à des actes de terrorisme ».

français ou européen est en route et nous espérons que ce dernier pourra contribuer à la sécurisation des données des villes intelligentes

L'éthique est désormais devenue un élément central dans la gestion des données issues des villes intelligentes. La réglementation doit maintenant se saisir du sujet de manière exhaustive afin de garantir l'utilisation dans de bonnes conditions des données collectées et d'en fixer les limites.

Nous pouvons citer également la ville de Nantes sur ce sujet qui a mis en place une charte de la donnée métropolitaine.

Cette charte s'articule autour de 4 engagements.

- Renforcer la protection des données.
- Mettre en œuvre des garanties.
- Agir avec sobriété.
- Garantir la transparence démocratique.

Les actions mises en avant passent par l'obtention de certification ISO27001, par la transparence sur les centres d'hébergement de données utilisées et par l'utilisation de produits et services qualifiés par l'ANSSI.
Elles sont, de plus, appuyées par l'ouverture du portail de publication des données publiques permettant ainsi à tous les usagers qui le souhaitent de contrôler les données collectées.

Ces exemples démontrent la tendance désormais essentielle de communiquer sur l'éthique et les enjeux de souveraineté pour villes intelligentes.

1.5.2 Enjeux technologiques

Avant de parler des enjeux technologiques, il est nécessaire de reprendre les aspects infrastructures. En effet, les technologies employées par les villes intelligentes dépendent d'infrastructure et d'interconnectivité qui sont parfois très différentes selon les territoires. Les réseaux d'interconnexion qu'ils soient sans fils, fibrés ou encore cuivrés sont le ciment des communications. Les flottes de dispositifs des villes intelligentes doivent être pilotables, administrables et mesurables simplement et avec une qualité de service irréprochable.

Les difficultés d'apporter des solutions d'interconnectivité en zone urbaine dense sont réelles. Déployer un réseau sans fil dans un espace avec des perturbations électromagnétiques et des saturations des bandes passantes radio est un réel challenge. Et c'est souvent la course à la puissance qui l'emporte. Pour pouvoir disposer d'une porteuse correcte, on augmente la puissance des dispositifs et ainsi leur consommation.

Un autre aspect à prendre en compte est l'interopérabilité des systèmes d'information des villes. En effet, le fonctionnement empirique en silo des organisations pousse à créer des systèmes d'information « métier » sans aucune gouvernance commune. Dans le monde de l'informatique de gestion, il existe des briques technologiques (ESB) permettant d'interconnecter des silos logiciel métiers différents. L'idée est que chaque système est à la fois producteur et consommateurs de données. Par exemple, nous pouvons imaginer un système de péage urbain permettant de réguler les entrées au sein d'une métropole qui en fonction de la localisation du propriétaire du véhicule définit des tarifs différents, avec des déclinaisons tarifaires également sur les caractéristiques des véhicules (pollution, taille, etc.). Ces systèmes sont déjà en place dans plusieurs métropoles des États-Unis. Le système de péage seul est à la fois producteur de données (flux de passage, tonnage de camion, régularité des transports en commun, etc…) et consommateurs de données (identité du propriétaire du véhicule, classe de véhicule, etc.).

Les enjeux technologiques liés à l'interconnexion des réseaux métiers sont donc essentiels, car chaque fournisseur de solution utilise des protocoles de communications différents voire parfois même propriétaire. Il n'existe pas aujourd'hui de consensus sur les technologies employées. Il appartient donc aux villes intelligentes de résoudre ces difficultés en proposant des canevas de technologies et des catalogues d'emplois de moyens de communication utilisable. Malheureusement lorsque l'on consulte les marchés publics et appels d'offres liés aux villes intelligentes, c'est rarement le cas.

Nous pouvons également remarquer l'arrivée de nouvelles technologies qui apporte un challenge pour les villes intelligentes. L'acceptation de celles-ci vient se superposer aux technologies actuelles créant ainsi un « mille-feuille technologique » favorisant peu leur contrôle, cela essentiellement dû à la complexité induite. Nous pouvons lister les technologies

suivantes qui transformeront nos vies quotidiennes car leurs applications et les nouveaux usages qu'ils généreront sont difficilement prédictibles :

- L'IoT, l'IA et le Big Data sont utiles pour automatiser la prise de décision, la résolution de problèmes et le développement de villes encore plus intelligentes ;
- La block-chain augmente la confiance dans les échanges de données devenant ainsi une plate-forme de communication sécurisée et proposant une meilleure résilience.

Ces technologies auront un impact majeur sur les villes, à la fois au niveau de la configuration physique et au niveau opérationnel. Elles doivent s'adapter à la diversité des problèmes et aux besoins des citadins, à la variété de l'environnement et doivent ainsi posséder un certain degré de transparence.

1.5.3 Enjeux juridiques

Il est impossible d'évoquer les enjeux juridiques sans rappeler les 3 grands thèmes gravitant autour de ces enjeux.

La protection des données personnelles avec le RGPD (règlement général sur la protection des données) est la clé de voute de l'arsenal législatif actuel. La manière dont les villes intelligentes traitent les données peut causer des problèmes aux administrations si des mesures adéquates ne sont pas adoptées. Ce cas est d'autant plus vrai que le RGPD est entré en vigueur depuis mai 2018.Il a été conçu pour harmoniser les lois sur la protection de la vie privée à travers l'Europe.

Les règles du RGPD sont une évolution positive pour les villes et les citoyens. Elles fournissent une clarté indispensable sur l'objectif de la collecte de données personnelles, la manière dont les données sont utilisées et la durée de leur conservation.

Il donne aux citoyens plus de contrôle sur leurs données personnelles et la possibilité de se retirer à tout moment. Ces règles mettent en place des garanties et des droits bien meilleurs pour les citoyens.

Le statut juridique des données est un élément difficile à déterminer ainsi que la propriété. Par exemple, la notion de donnée d'intérêt général a été introduite par la loi « Lemaire » pour une République numérique. Ces données sont définies comme : « *les données et les bases de données collectées ou produites à l'occasion de l'exploitation du service public faisant l'objet du contrat et qui sont indispensables à son exécution* ». Ainsi, il incombe désormais au

concessionnaire de fournir à l'autorité concédante sous format électronique, les données et les bases de données collectées ou produites à l'occasion de l'exploitation du service public faisant l'objet du contrat, afin de permettre à celle-ci de remplir les obligations.

La loi sur la transition énergétique pour la croissance verte a introduit de nouvelles dispositions ayant pour objet d'imposer l'ouverture des données aux gestionnaires du réseau public de transport d'électricité, de distribution d'électricité, des réseaux du gaz et des réseaux de chaleur.

Cependant, avec le monopole d'Enedis et de GRDF, les données du secteur de l'énergie se heurtent à deux obstacles.

- refus de transmission des données personnelles ;
- refus de transmission des informations commercialement sensibles.

La réticence de ces deux opérateurs est un enjeu pour les projets de smart grid et, plus largement, pour les pratiques innovantes de gestion des données énergétiques. Autant pour les données personnelles, il est possible de faire sans car les données peuvent être anonymes. En revanche, l'optimisation tarifaire et les objectifs de consommations sont protégés par le code de l'énergie, articles L111-73 et -81 et le décret n°2001-630 du 16 juillet 2001.

1.5.4 Enjeux financiers

Les projets de smart-city englobent souvent de nombreuses couches technologiques et font appel à de multiples compétences. Les investissements sont bien souvent importants et nécessitent de revoir les budgets à la hausse.

On peut distinguer deux « générations » de ville intelligente. La première se caractérise par la présence d'opérateurs urbains historiques. Ceux-ci interviennent dans l'optimisation des flux et des processus autant dans le domaine de l'infrastructure urbaine (Veolia, Engie, Vinci) que dans celui des technologies et de l'informatique (Orange, Huawei, Microsoft, IBM, Cisco). Ces acteurs sont présents à travers les marchés publics et proposent leurs technologies pour améliorer l'efficacité des services qu'ils supportent. On parle alors d'usager-consommateur.

La seconde génération est beaucoup plus récente et se caractérise par le fait que les services numériques s'adressent directement aux utilisateurs finaux. Ces entreprises issues du monde numérique (Google, Citymapper, Waze, Placemeter, Uber) proposent une vision relationnelle de la ville numérique. Les services sont souvent gratuits pour l'usager et se financent via

l'exploitation des données générées par leur usage. Le passage par la case « marchés publics » n'est pas la logique suivie par ces acteurs qui par conséquent disruptent les enjeux et la relation entre les usagers et les collectivités.

Afin de financer les projets, la Caisse des dépôts (CDC) repère les projets d'investissement qui ont un apport pour l'intérêt général et propose des financements en amont et accompagne les collectivités.

Ainsi la Caisse des dépôts et ses filiales (Egis, Transdev, Icade, SNI) sont à l'initiative de programmes smart city :

- Deux en Île-de-France : le village olympique (sur les territoires de L'Ile-Saint-Denis ; Saint-Ouen et Saint-Denis) et Plaine Commune (Porte d'Aubervilliers) ;
- Six en régions : Bordeaux, Toulouse, Nice, Lyon, Besançon, Nantes.

Du côté de l'Europe, nous pouvons lire dans le rapport sur le financement des Smarts Cities de France stratégie : « la Banque européenne d'investissement accompagne plus de 450 projets chaque année et a ainsi accordé 83,3 milliards d'euros de prêts en 2016 investis à 90 % sur le sol européen. Elle finance des projets incluant une dimension environnementale forte, portant aussi bien sur des enjeux d'infrastructures urbaines que d'innovations technologiques ou de soutien aux PME ».

1.5.5 Enjeux de sécurité

Loin d'être anecdotique, la sécurité est un enjeu transversal incluant tous les domaines de la vie quotidienne. Nous avons vu précédemment que les enjeux autour de la donnée, de sa propriété et du respect de la vie privée sont au cœur des préoccupations des usagers des villes intelligentes.

Aujourd'hui, il n'existe pas de référentiel de sécurité ou de consensus sur la gouvernance de celle-ci. Nous ne sommes encore qu'au début d'une ère numérique où le quotidien des espaces urbains sera grandement modifié. Nous pouvons toutefois noter certaines initiatives sur des sujets connexes aux smart city mais qui côtoient les mêmes enjeux. Le gouvernement britannique a récemment mis en ligne un appel à contribution pour la régulation de la cybersécurité dans le domaine de l'internet des objets. Elle est axée sur 4 thèmes :

- Protéger les citoyens, les réseaux et les infrastructures.
- Permettre aux technologies émergentes de se développer et de prospérer en améliorant la sécurité et en augmentant la confiance des consommateurs.
- Adopter une approche proportionnée pour imposer des obligations aux acteurs économiques concernés, sans compromettre l'efficacité.
- Continuer à protéger les citoyens, les réseaux et les infrastructures contre les préjudices face à un avenir incertain.

Nous sommes clairement sur les thèmes et les enjeux des villes intelligentes. Il sera intéressant de consulter les publications et leurs applications dans le futur.

Nous pouvons également souligner le travail de l'ANSSI à destination des collectivités territoriales. Ainsi, « *Pour répondre au défi de la sécurité du numérique des collectivités territoriales, la France, soit directement par son droit national soit via les règlements et directives pris au niveau de l'Union Européenne, s'est dotée d'un cadre règlementaire participant à la protection de ces systèmes d'information et dont les objectifs sont :*

- Le renforcement de la confiance des usagers dans l'utilisation des services numériques.
- Le renforcement de la sécurité des données à caractère personnel.
- La transformation numérique des administrations l'État.
- Le renforcement de la sécurité des acteurs critiques pour l'État. ».

Nous pouvons constater que le sujet préoccupe beaucoup les autorités. L'évolution est rapide et le volet réglementaire et sécurité peine aujourd'hui à répondre aux enjeux.

Pour la France, l'objectif est de sensibiliser, former et éduquer les collectivités aux enjeux de cybersécurité en se basant sur les textes de lois existantes :

Figure 14 : les collectivités face aux enjeux de cybersécurité - infographie - ANSSI

Ici il est question de présenter les textes de références et d'aider à leur compréhension. Pour l'ANSSI, le découpage des enjeux de sécurité suit 3 thèmes : les téléservices, les données personnelles et les systèmes d'importances vitales.

Concernant les téléservices, les objectifs sont de conduire une analyse de risques et de définir les mesures de sécurité adaptées aux enjeux et aux menaces, puis l'homologation de sécurité du téléservice et enfin le suivi opérationnel et l'amélioration continue. Le texte applicable est le RGS (Référentiel Général de Sécurité).

Pour les données personnelles, nous en avons déjà évoqué ces aspects dans la section sur les enjeux juridiques cependant les objectifs sont la nomination d'un délégué à la protection des

données puis l'établissement d'un registre de traitement. Viennent ensuite l'analyse d'impact, la mise en place des clauses relatives à la protection des données personnelles avec ses fournisseurs et ses sous-traitants et les notifications des violations de données personnelles.

Enfin, les systèmes d'informations d'importance vitale ou essentiels (SIIV) ou les systèmes d'information essentiels sont encadrés par la loi de programmation militaire dans son article 22[15] et la directive NIS. Ces réglementations visent à définir un cadre en matière de cybersécurité pour les opérateurs d'importance vitale, aux opérateurs de services essentiels et aux fournisseurs de services essentiels.

Ces réglementations portent sur les domaines suivants :

- La gouvernance de la sécurité des réseaux et systèmes d'information, sur l'élaboration et la mise en œuvre d'une politique de sécurité des réseaux et systèmes d'information et l'homologation de sécurité des réseaux et systèmes d'information.
- La protection des réseaux et systèmes d'information, sur la sécurité de l'architecture et de l'administration des réseaux et systèmes d'information et le contrôle des accès à ces réseaux et systèmes.
- La défense des réseaux et systèmes d'information, sur la détection et le traitement des incidents de sécurité affectant les réseaux et systèmes d'information.
- La résilience des activités, sur la gestion de crises en cas d'incidents de sécurité ayant un impact majeur sur des services essentiels.

Des sanctions (financières, administratives et pénales) sont également prévues en cas de non-respect de la réglementation.

1.5.6 Enjeux de résilience

La résilience - pour les villes comme pour les organisations - est devenue une priorité à la suite de la pandémie. Le terme reflète la capacité d'une ville à assurer la continuité des services pour la ville et les citoyens en cas de catastrophe, à se reconstruire rapidement et à prospérer après l'événement. Des niveaux élevés de résilience urbaine reposent sur des infrastructures de qualité, des communautés interconnectées et une bonne gouvernance. Lorsque ces éléments sont liés les uns aux autres, les villes peuvent faire face et rebondir rapidement même après la crise la plus difficile.

[15] loi n° 2013-1168 du 18 décembre 2013.

La cybersécurité joue un rôle essentiel dans l'atténuation des chocs et des stress en protégeant la confidentialité, l'intégrité et la disponibilité des données et des infrastructures activées par les données. Cependant, la sécurité seule ne suffit pas. La cyber-résilience va encore plus loin en veillant à ce que les systèmes TIC continuent de fournir des services en cas de faille de sécurité. Pour les villes, la cyber-résilience peut être comprise à travers leur capacité de préparation, de réponse et de réinvention. Les efforts visant à renforcer la cyber-résilience sont essentiels pour survivre et même potentiellement prospérer face aux cyberattaques ou aux catastrophes physiques.

Les villes ne seront jamais « sécurisées » à 100% et ne pourront éviter complètement le danger. Mais ils peuvent être résilients face à un large éventail de stress et de chocs en faisant les bons investissements, à la fois dans les domaines physiques et cybernétiques, pour se préparer aux crises, réagir pour rétablir la normalité, apprendre du nouveau statu quo et s'y adapter.

Afin d'aider les villes à devenir plus résilientes physiquement, socialement et économiquement face aux menaces, l'une des mesures que les villes peuvent prendre est d'embaucher un responsable de la résilience.

Aujourd'hui, la plupart des villes ne disposent pas encore du personnel nécessaire pour élaborer une stratégie efficace. En tant que tel, il est important dans un premier temps d'embaucher un gestionnaire possédant une expérience pertinente qui sera en mesure de poser les bonnes questions, d'examiner le fonctionnement actuel des agences et de concevoir une stratégie qui prend en compte la situation unique de la ville.

Chaque ville est différente. Comprendre les menaces de cybersécurité importantes et uniques pour une ville particulière, ainsi que leur impact potentiel, est essentiel pour garantir que la ville puisse y répondre efficacement. Par exemple, une ville qui dépend fortement des ponts pour la sortie sera confrontée à des questions de résilience différentes pour ses systèmes de circulation que celle dont les routes sont plus dispersées. Cette clarté permet à la ville d'identifier et de planifier les niveaux d'efforts et d'investissements nécessaires en matière de cybersécurité.

Chaque ville s'appuie sur des services critiques et des informations sensibles qui, si elles étaient compromises, endommagées ou détruites, auraient un impact dramatique sur la capacité de la ville à fonctionner. Celles-ci doivent être identifiées puis hiérarchisées, ce qui implique souvent des compromis difficiles, mais il est essentiel que la ville puisse réagir

efficacement en cas de crise. Par exemple, aux États-Unis, le National Institute of Standards and Technology (NIST) propose des ressources faisant autorité, notamment les « Standards for Security Categorization of Federal Information and Information Systems » et le cadre « Protecting Critical Infrastructure Cybersecurity », qui peuvent aider les villes à faire décisions de sécurité fondées sur les risques.

Une fois les menaces et les services critiques identifiés, la ville doit définir sa vision de la cyber-résilience. Sur cette base, il peut s'engager dans un effort de collaboration pour fixer des objectifs qui décrivent les objectifs spécifiques qu'ils souhaitent atteindre. Ces objectifs peuvent inclure de garantir que la ville dispose d'une plate-forme de données ouvertes efficaces qui peut fournir des informations aux premiers intervenants en cas d'urgence (chocs aigus) ou d'aider les organismes sans but lucratif à mieux répondre aux besoins des résidents de la ville au quotidien (facteurs de stress constants).

Malheureusement, nous vivons dans un monde où il ne s'agit pas de savoir si ces événements se produiront, mais quand. Il est donc essentiel que les villes spécifient les résultats souhaités pour la ville après une crise, puis identifient les capacités nécessaires pour répondre à ces événements. Dans le monde physique, les villes à haut risque de tremblement de terre ont conclu des accords de niveau de service avec leurs citoyens - par exemple, elles savent quel pourcentage de bâtiments peut être déblayé par les sauveteurs dans les 24 heures. Les mêmes résultats et accords devraient être élaborés pour les cyber-risques.

Enfin, la ville doit examiner ses principales menaces, priorités, objectifs et résultats et identifier les ressources nécessaires pour concrétiser la vision de la cyber-résilience. L'effort doit porter sur les personnes, les compétences, la technologie et le financement, ainsi que sur la cartographie des responsabilités pour les actions à entreprendre à la fois naturellement et en cas de violation de la cybersécurité.

1.5.7 Enjeux de la gouvernance des données

La donnée est au cœur de la smart city à en être devenue un véritable prérequis à son développement. Même si les différentes expérimentations actuelles démontrent déjà une certaine capacité à capter et exploiter ces données, il semble plus que nécessaire d'en accentuer la maitrise et d'en organiser de façon pertinente la gouvernance.

Les villes intelligentes ne pourront continuer à se développer sans cette démarche de redéfinition des interactions et du traitement des données entre les différents acteurs de la vie urbaine (privés, publics, consommateurs, citoyens). La gestion des données constitue donc un enjeu stratégique pour la démocratie locale, la gestion du territoire et le développement économique.

Il devient alors nécessaire de partager et gérer des données de façon intelligente.La transformation numérique de la ville se met au service du citoyen et du développement durable. Selon la CNIL, l'ambition de la Smart City est « d'améliorer la qualité de vie des citadins en rendant la plus adaptative et efficace, à l'aide de nouvelles technologies qui s'appuient sur un écosystème d'objets et de services ».

Cette transformation est déjà en marche dans de nombreuses villes à travers le monde et beaucoup de solutions sont déjà déployées et opérationnelles.

Figure 15 : Quelques exemples de solutions Smart City déployées dans le monde (spinpart.fr)

Même si de nombreuses solutions techniques de traitement de la donnée existent, l'enjeu est de pouvoir les déployer à grande échelle et surtout d'en assurer l'interopérabilité. La complexité réside également dans l'intégration de ces solutions dans l'écosystème technique et organisationnel déjà en place. Il est alors nécessaire de définir les rôles et périmètres de chacun, notamment qui possède la donnée générée et qui accède à l'information.

Le challenge de la gouvernance de ces données est d'avoir la capacité à traiter la richesse des données collectées, toujours plus nombreuses et variées (bâtiments, réseaux (électricité, gaz, eau, chaleur), objets connectés (IoT) incorporés au mobilier urbain, capteurs sociaux, etc.) également de savoir comment croiser des données brutes d'acteurs différents, parfois concurrents, tout en en protégeant l'accès et la propriété.

La donnée devient alors un nouveau bien commun et ses sources sont maintenant multiples : objets connectés, réseaux sociaux, saisies informatiques, relevé terrain, capteurs. Ces données sont ensuite acheminées et stockées dans des bases de données toujours plus grandes et deviennent ainsi consultables en accès libre (Open Data) ou privé. Le développement des plateformes de données devient donc de plus en plus primordial ainsi que l'organisation des données publiques, toujours plus riches.

En 2016, la loi pour une république numérique lance le service public de la donnée et introduit la notion de données d'intérêt général (DIG). De ce fait les collectivités de plus de 3 500 habitants, ainsi que les délégations de service public (DSP) sont maintenant dans l'obligation de publier en open data l'ensemble des données non sensibles générées dans le cadre de leur mission de service public.

Mais cette publication peut aller plus loin encore jusqu'à intégrer l'ensemble des données présentes sur le territoire de la collectivité concernée, et ce jusqu'aux données privées. Il devient alors nécessaire de développer des projets de plateforme.

Voici quelques exemples de solution d'intégration, de centralisation et de mise à disposition de ces données par un tiers de confiance :

- La ville de Lyon avec sa plateforme data.grandlyon.com.
- La solution 3DEXPERIENCity de Dassault Systèmes à Rennes.
- La plateforme MUSE à Dijon.
- La Plateforme Régionale d'Innovation pour les Données d'Energie (PRIDE) développée par consortium d'acteurs privés pour les régions Bretagne et Pays de Loire.

Restant la propriété de ceux qui les injectent dans le système, les données peuvent alors être partagées par tous et ainsi permettre le développement de nouveaux services.

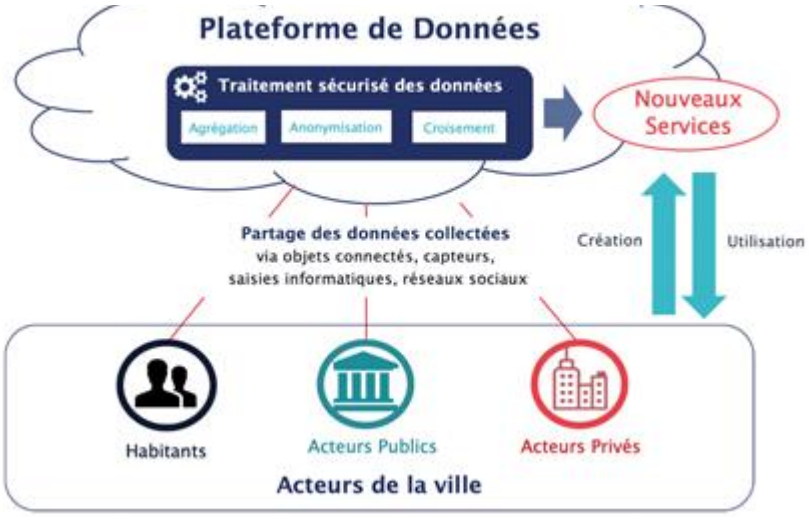


Figure 16: Cas d'usage des plateformes de données (spinpart.fr)

L'animation de ce nouvel écosystème autour de la donnée pour l'essor des smart city (ouverture, partage, hébergement, interfaçage et utilisation) est essentielle et incombe aux collectivités territoriales :

- Incitation aux partages des données par les déférents acteurs (privés ou publiques) ;
- Respect de la vie privée des individus.
- Maitrise des données et assurer une indépendance par rapport aux plus grands acteurs privés de la donnée.
- Création de nouveaux services correspondants aux besoins des usagers.
- Négociation et intégration des données dont elles ne sont pas propriétaires (exemple de la ville de Paris qui a dû négocier avec des acteurs privés tels que Uber, Lime ou encore Waze pour l'intégration de leurs données au sein de sa plateforme « Connected Citizen »).

On note alors que les collectivités locales ont besoin de se réinventer afin de pouvoir piloter la donnée locale de façon stratégique et efficace. Elles doivent relever certains nouveaux défis tels que :

- Développer des compétences techniques digitales.
- Réorganiser les services et les équipes de façon à ne plus fonctionner en silo, mais en transversalité.
- Introduire la notion d'expérimentation et créer de nouveaux partenariats avec les différents acteurs de l'écosphère smart city.

Mais une fois tout cela mis en place et comme la CNIL l'indique avec la notion de smart citizens, la réussite de la smart city réside dans l'intégration de l'individu c'est-à-dire à placer l'humain au cœur du système.

2 RISQUES SMART CITIES

2.1 RISQUES ET IMPACTS POUR LES CITOYENS

Au cours des dernières décennies, les réseaux d'infrastructures urbaines ont eu tendance à utiliser les TIC pour essayer de résoudre les problèmes urbains afin de fournir des services plus pertinents. Ces efforts s'inscrivent désormais dans le concept de villes intelligentes en tant que mouvement mondial qui cherche à transformer et faciliter la gestion et la vie urbaine grâce à l'utilisation des nouvelles technologies. Ce phénomène permettra de résoudre les problèmes de résilience et de durabilité urbaines à une époque marquée en particulier par une augmentation rapide de la population et des changements environnementaux. En d'autres termes, les technologies des villes intelligentes sont considérées comme un moyen efficace pour offrir des services aux citoyens, mais également pour gérer l'incertitude et le risque en fonction des infrastructures que les villes ou États vont déployer.

Cependant, comme les cycles précédents d'adoption et d'adaptation technologiques dans les villes, ils créent une situation contradictoire où les bénéfices promis tels que l'accessibilité, les gains économiques, la sécurité, la durabilité s'accompagnent de conséquences imprévues et de nouvelles variations des problèmes traditionnels (par exemple, la reproduction des inégalités, la création de risques sécuritaires et criminels, etc.). Cette situation contradictoire est pour la plupart ignorée dans le discours officiel des responsables en charge de ces projets de villes intelligentes qui sont motivés par des intérêts commerciaux et enjeux

Dans la suite du document, nous examinerons en profondeur cette relation paradoxale, en détaillant comment les technologies des villes intelligentes conçues pour produire une résilience urbaine et réduire les risques ouvrent en réalité les systèmes urbains qu'elles sont censées améliorer à de nouvelles formes de vulnérabilités et de risques. En particulier, nous sommes intéressés par l'examen du point d'équilibre entre la récompense et le risque lorsque des systèmes auparavant relativement "autonome" sont rendus "intelligents" par l'introduction de l'informatique en réseau, et sont donc ouverts aux bugs logiciels, aux erreurs de données, aux virus de réseau, aux piratages et aux entreprises criminelles et terroristes. Nous nous intéressons particulièrement aux vulnérabilités de sécurité et à la mesure dans laquelle il devient possible de pirater et de perturber les technologies des villes intelligentes et de commettre de nouvelles variantes d'activités criminelles.

Comme le décrit la littérature en plein essor sur la criminalité et la ville, depuis qu'il existe des sociétés urbaines, il y a toujours eu des activités criminelles et des tentatives de pénétrer, d'attaquer, de frauder et de perturber les infrastructures et les services publics des villes.

Les tentatives de limiter et de se défendre contre ces crimes se sont intégrées dans le tissu des villes elles-mêmes par le biais de défenses édictées par l'architecture, de portes solides, de serrures, de grilles de fenêtres, de hauts murs et de clôtures, d'alarmes de sécurité et de vidéosurveillance. Cependant, l'histoire a montré que toutes ces mesures de sécurité présentent certaines vulnérabilités que les criminels sont prompts à identifier et à exploiter. Avec le temps, toutes les sécurités, même les solutions sophistiquées ou bien conçues, seront contournées (surtout si la récompense du succès fournit une motivation suffisante). Il y a donc une lutte perpétuelle entre les défenseurs et les attaquants pour sécuriser les systèmes qui fournissent une protection adéquate.

Les technologies intelligentes ne font pas exception à la règle, car elles sont affectées par toute une série de vulnérabilités et de risques en matière de sécurité, et une lutte permanente est désormais évidente entre l'industrie de la cybersécurité, les criminels et les pirates informatiques aux motivations diverses. Cependant, si les motivations pour pénétrer dans ces systèmes restent intemporelles (par exemple, vol, extorsion, usurpation d'identité, vandalisme, attaque malveillante), la nature de leurs performances est différente.

Comme ces technologies reposent sur des logiciels et des systèmes en réseau, l'exploitation de leurs vulnérabilités peut se faire à distance et les attaques peuvent être masquées, ce qui réduit le risque de détection et d'identification des auteurs. En outre, l'utilisation d'outils pour automatiser le piratage a considérablement réduit les coûts et a donné aux pirates le pouvoir de mener des activités criminelles contre plusieurs cibles simultanément, ce qui peut affecter de nombreuses villes différentes.

La surface d'attaque désigne l'ensemble des façons dont un système peut être sensible à une attaque, on parle également parfois de surface d'exposition. Ces expositions sont multiples en raison des nombreuses parties imbriquées des systèmes, qui sont détenues et contrôlées un ensemble diversifié de parties prenantes rendant difficile leur sécurisation et augmentant ainsi les accès non autorisés. Les récompenses en cas de succès sont souvent spectaculaires, par exemple dans le cas d'une violation de données donnant accès à des millions

d'informations sur des utilisateurs, lors d'un acte de vandalisme ou de terrorisme entraînant la coupure de l'ensemble de l'approvisionnement en électricité d'une ville.

2.2 FORMES DE CYBERATTAQUES ET FACTEURS D'AMPLIFICATION

Les cyberattaques visent à "*altérer, perturber, tromper, dégrader ou détruire des systèmes et réseaux informatiques ou les informations et/ou programmes qui y résident où y transitent*".

Il existe trois formes distinctes de cyberattaques contre les systèmes opérationnels : les attaques qui visent à rendre indisponible un service ou un système ; les attaques avec l'exfiltration de données ; et les attaques touchant l'intégrité des données. Les cyberattaques peuvent être menées par de multiples acteurs différents, qu'il s'agisse d'agences de renseignement étatiques, de groupes terroristes, de criminels organisés, de collectifs de pirates informatiques, de militants politiques et sociaux ou de pirates informatiques " ou encore de "script kiddies[16]".

De manière générale, les attaques informatiques tentent d'exploiter l'une des cinq principales vulnérabilités des technologies qui sont au cœur des systèmes des villes intelligentes.

La première d'entre elles est la faiblesse de la sécurité dans le développement des logiciels. Des recherches menées par une équipe de l'université Carnegie Mellon en 2004 ont montré qu'il y a en moyenne trente erreurs ou bogues potentiellement exploitables pour 1 000 lignes de code. Dans les infrastructures principalement déployées dans les villes intelligentes, il y a des millions de lignes de code qui produisent des milliers d'exploits *zero-day* potentiels (vulnérabilités de sécurité encore inconnues). En outre, des recherches menées par divers spécialistes en sécurité ont détaillé comment de nombreux systèmes intelligents ont été construits sans intégrer la sécurité dès la phase conception du composant ou produit (en anglais : Security by design, SBD).

À titre d'exemple, en utilisant le moteur de recherche Shodan, il est possible d'identifier toutes sortes de dispositifs informatiques et de systèmes de contrôle connectés directement à Internet - des thermostats en réseau pour les systèmes de chauffage aux systèmes de contrôle de la circulation et aux centres de commande et de contrôle pour les centrales nucléaires - dont beaucoup se sont avérés n'avoir que peu ou pas de sécurité. De plus, les municipalités et les vendeurs de technologies de villes intelligentes les déploient souvent sans entreprendre de tests de sécurité préalable.

[16] Une personne non qualifiée qui utilise des scripts ou des programmes développés par d'autres pour attaquer les systèmes et réseaux informatiques.

La deuxième vulnérabilité concerne l'utilisation de systèmes plus anciens non sécurisés et peu ou pas maintenus. En effet, de nombreuses technologies sont superposées à une infrastructure bien plus ancienne qui repose sur des logiciels et des technologies installées depuis plusieurs décennies qui ne sont plus mises à jour voire maintenables. La troisième vulnérabilité provient des dispositifs numériques des villes intelligentes eux même qui sont généralement étendus, complexes et diversifiés, avec de nombreuses interdépendances et par conséquent des surfaces d'attaque importantes et complexes. Bien que les systèmes indépendants soient sécurisés, les relier à d'autres peut potentiellement les fragiliser ; le niveau de sécurité n'étant garanti que par le maillon plus faible. Au-delà du piratage, la complexité des systèmes augmente également les chances d'accidents plus classiques (par exemple, les bogues de programmation, les erreurs humaines) qui provoquent des défaillances imprévues.

Les interdépendances entre les technologies et les systèmes des villes intelligentes induisent un risque de créer des effets en cascade en cas d'attaque informatique. Par exemple, une cyberattaque sur une infrastructure d'énergie électrique pourrait se répercuter en cascade sur un système d'exploitation urbain qui se répercute ensuite sur les autres systèmes tels que la gestion du trafic, les services d'urgence et les services d'eau. En effet, il s'agit de l'un des principaux risques en matière de sécurité et de résilience d'un système d'exploitation urbain, dans lequel plusieurs systèmes sont reliés entre eux pour permettre une approche "intégrée" de la gestion des services et des infrastructures de la ville, annulant ainsi les effets d'atténuation de l'utilisation d'une approche en silo. Une cyberattaque réussie sur le réseau électrique a d'énormes effets en cascade, car il sous-tend de très nombreuses activités telles que l'alimentation des foyers, des lieux de travail et d'une pléthore d'autres infrastructures essentielles. Par exemple, la cyberattaque sur le logiciel contrôlant certaines parties du réseau électrique ukrainien a coupé le courant à environ un quart de million de consommateurs pendant plusieurs heures en décembre 2015.

Quatrièmement, il existe de multiples vulnérabilités découlant de l'erreur humaine et de la malveillance (ex : employés mécontents). Les exploits techniques peuvent être considérablement favorisés par l'erreur humaine, par exemple, l'ouverture de courriels d'hameçonnage ou l'installation de logiciels malveillants. Dans d'autres cas, les logiciels de sécurité ne sont pas installés de manière appropriée, les codes d'accès (par défaut) ne sont pas modifiés ou la sécurité du système n'est pas tenue à jour.

Enfin, les cybercriminels sont capables de réaliser de l'ingénierie sociale sur des employés, par exemple en utilisant l'hameçonnage pour collecter des informations clés (par exemple, des noms d'utilisateur et des mots de passe) qui facilitent l'accès. De même, les révélations de Snowden prouvent également que des "initiés" ont été placés par des agences de renseignement d'État dans l'intention de compromettre délibérément la conception du matériel de mise en réseau et les paramètres fondamentaux du système afin de faciliter l'espionnage électronique, le sabotage et la cyberguerre.

Ces vulnérabilités sont accentuées par un certain nombre de causes, notamment le fait qu'il est souvent difficile de savoir qui est responsable du maintien de la sécurité dans les systèmes et les infrastructures complexes lorsque plusieurs entreprises et parties prenantes collaborent à leur conception, fournissent du matériel et des logiciels, et exploitent et utilisent divers éléments. Cette situation est amplifiée en ce qui concerne la gestion urbaine, où les municipalités sont soumises à une pression croissante pour réaliser des économies d'efficacité d'année en année, qui affectent la sécurité de trois manières :

- Premièrement, il existe un sous-investissement dans la maintenance des infrastructures et une dépendance excessive à l'égard des systèmes existants.
- Deuxièmement, la difficulté pour les organisations du secteur public de recruter du personnel informatique qualifié et motivé pour mettre en œuvre et maintenir correctement les technologies des villes intelligentes.

La maintenance informatique fait de plus en plus appel à des entrepreneurs indépendants et à des services externalisés, ce qui, d'une part, déqualifie les capacités internes et érode la mémoire institutionnelle dans le secteur public et, d'autre part, crée une responsabilité distribuée avec un ensemble fragmenté d'organismes (avec des services sous contrat, des accords de niveau de service, des équipes multi-agences et des services d'assistance à distance) qui supervisent la sécurité, ce qui entraîne souvent un manque de continuité, de coordination et de responsabilité.

Troisièmement, il y a un manque d'investissement dans le personnel informatique dédié à la sécurité et dans les équipes en réponse sur incident informatique. L'expertise en matière de sécurité informatique est souvent limitée à une poignée d'individus peu ou pas formée à la sécurité de ces technologies émergentes (ce qui augmente la probabilité d'erreur humaine). Les plans de sécurisation dont disposent les villes sont souvent cloisonnés par rapport à des

systèmes et des services particuliers, de sorte que l'évaluation et la réponse transversales font cruellement défaut. De nombreux fournisseurs de villes intelligentes ont peu ou pas d'expérience dans l'intégration de fonctions de sécurité dans leurs produits - malgré les déclarations faites dans leur documentation commerciales - et de nombreux systèmes présentent des failles importantes nativement.

Certains fournisseurs sont susceptibles d'entraver la recherche en matière de sécurité en limitant l'accès à leurs systèmes pour les tester, ce qui leur permet de continuer à commercialiser des produits non sécurisés sans surveillance ni responsabilité. De même, trop de villes ont fait preuve de laxisme en insistant sur des contrôles et des réponses de sécurité solides dans le cadre du processus d'acquisition de nouveaux systèmes.

Ces formes de cyberattaques et les facteurs d'amplification signifient que les technologies et infrastructures des villes intelligentes présentent un certain nombre de vulnérabilités et de risques de sécurité susceptibles d'être exploités.

2.3 VULNERABILITES ET RISQUES DE SECURITE DES VILLES INTELLIGENTES

Dans cette partie, nous détaillons des exemples dont des dispositifs spécifiques ont été, ou pourraient être, compromis, illustrant l'ampleur et l'impact potentiels de telles attaques informatiques. Certains de ces évènements redoutés que nous avons identifiés sont principalement liés à l'avènement des nouvelles technologies numériques et peuvent s'appliquer à des instances beaucoup plus vastes que la ville intelligente elle-même. Ce que nous voulons explorer dans ce chapitre, c'est le paradoxe suivant : le principal outil sur lequel se fonde la ville intelligente peut, dans nombreux cas, mettre en périls ses principaux objectifs.

2.3.1 Réseau électrique intelligent

Cette section se concentre sur l'infrastructure dans le secteur de l'électricité, qui fait partie d'une série de recherche sur la sécurité et la résilience. L'utilisation des technologies intelligences induit des risques :

- L'augmentation du degré de mise en réseau et d'automatisation des processus de production, de distribution, de transmission et de mesure dans le réseau électrique.
- L'introduction d'un grand nombre de périphériques physiques avec une connectivité réseau difficile à protéger. Beaucoup de ces périphériques interagiront directement avec les clients, élargissant ainsi la surface d'attaque et introduisant des variables difficiles à contrôler.

Les trois technologies qui font ou feront partie des futurs systèmes électriques sont : les centrales électriques intelligentes, la distribution et la transmission intelligentes, et l'infrastructure de comptage avancée.

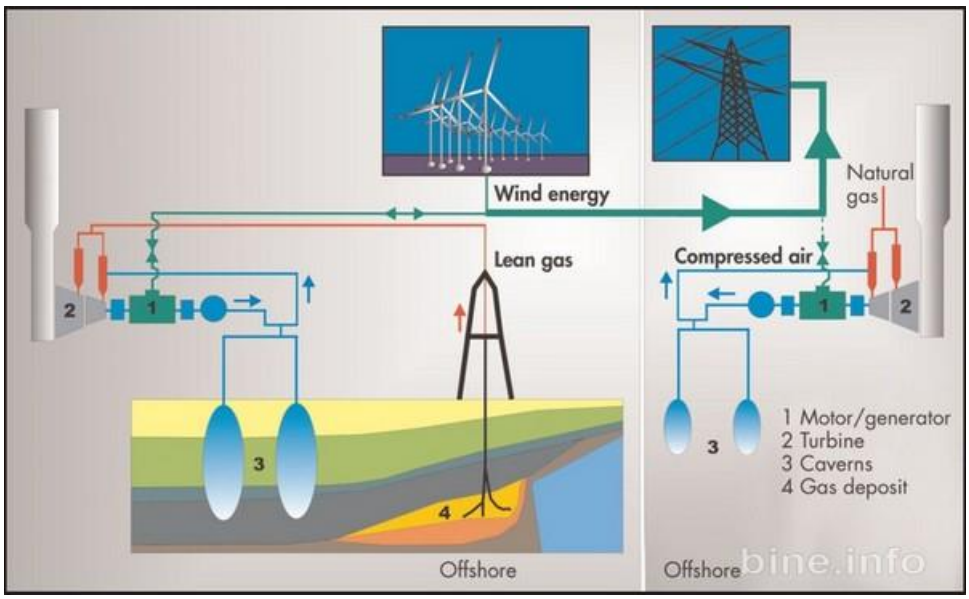


Figure 17 : Combinaison de technologie pour le stockage sous forme d'énergie mécanique (smartgrids.wordpress.com)

2.3.1.1 Les centrales électriques intelligentes

En raison du degré élevé de connectivité et d'automatisation des systèmes de production d'électricité intelligents, les acteurs malveillants qui peuvent tirer parti des faiblesses du système pourraient être en mesure de contrôler un grand nombre de composants clés dans un ou plusieurs systèmes, y compris les chaudières, les turbines, les pompes et les vannes. Le contrôle de ces composants peut être utilisé pour effectuer diverses opérations destructives, telles que la modification du débit de vapeur vers la turbine, la sous-alimentation ou la surcharge de la turbine, la rotation de la turbine sans lubrification nécessaire ou l'empêchement de l'eau de pénétrer dans le système pour le refroidissement. Les acteurs malveillants peuvent également recourir à des moyens nuisibles pour désactiver le système de contrôle et d'acquisition de données (SCADA) et d'autres fonctions à distance afin d'empêcher les interventions à distance. Le traitement des données peut être utilisé pour masquer la présence d'anomalies, augmentant ainsi la possibilité d'interférences ou d'impacts plus importants sur le système. La manipulation des données peut également être utilisée

pour fournir une lecture erronée des données, obligeant l'opérateur ou l'administrateur à prendre des mesures non valides ou dangereuses.

De même, ils pourraient également utiliser du matériel, des courriers électroniques ou des supports de transmission infectés pour introduire des logiciels malveillants conçus pour modifier divers paramètres du système de production d'énergie afin d'endommager la machine. Ces mêmes acteurs pourraient concevoir des logiciels pour localiser et manipuler des périphériques ou des systèmes logiciels spécifiques, attendre que l'attaque soit exécutée à un moment prédéterminé et rechercher des opportunités de propagation.

Les attaques contre les centrales électriques intelligentes pourraient avoir un impact important au niveau local ou régional si elles provoquent des pannes de courant ou des coupures permanentes, en particulier si une attaque vise plusieurs centrales en même temps. En outre, une panne d'électricité provoquée intentionnellement pourrait causer des dommages économiques importants, car de nombreuses entreprises seraient dans l'incapacité de fonctionner.

Les pannes annoncées comme résultant d'une attaque peuvent susciter la méfiance à l'égard des services publics et augmenter le risque de troubles ou de panique. Une attaque visant plusieurs centrales électriques intelligentes augmenterait la zone touchée et entraînerait des pannes plus longues, ce qui accroîtrait la probabilité de pertes de vies humaines et d'autres effets négatifs. Les effets d'une attaque visant le matériel physique seraient particulièrement problématiques, car certains composants de production ne disposent pas d'unités de rechange régulièrement disponibles en stock en raison de leur taille et de leur coût, et nécessitent également de longs délais de fabrication, d'expédition et d'installation.

2.3.1.2 Distribution et de transmission

Les systèmes de distribution sont conçus pour accroître notamment l'efficacité et la flexibilité globales du réseau intelligent, et réduire les erreurs de distribution et de transmission. Ces dispositifs comprennent l'installation de divers dispositifs d'automatisation ou de mise en réseau. Les systèmes de distribution et de transmission intelligents utilisent des systèmes SCADA et d'autres dispositifs d'automatisation pour augmenter les temps de réponse aux pannes de courant et pour recueillir plus rapidement des données sur les performances du réseau. De même, l'installation progressive de capteurs le long des lignes de distribution et de

transmission permet aux opérateurs de recueillir des informations sur l'utilisation en temps réel, de mieux intégrer la production d'énergie renouvelable intégrée au réseau et d'isoler les interruptions de système avant qu'elles ne se propagent.

Les capteurs en réseau sur les transformateurs permettent aux opérateurs de suivre les performances des équipements et de mieux anticiper les défaillances, ce qui réduit les pannes et les coûts de réparation. Enfin, l'augmentation des réseaux de communication dans les systèmes de distribution et de transmission améliorera l'intelligence globale du système, ce qui permettra de mieux intégrer les programmes de réponse à la demande, qui permettent aux clients de suivre la disponibilité et le prix de l'énergie pour prendre des décisions de consommation en conséquence.

Bien que les systèmes de distribution et de transmission soient composés de multiples éléments, des attaques visant plusieurs éléments individuels pourraient être exécutées pour endommager le matériel ou provoquer des pannes et des coupures de courant à l'échelle du système.

Par exemple, une attaque coordonnée visant les réseaux SCADA et de communication à grande échelle associée à plusieurs sous-stations de transmission, pourrait permettre aux auteurs de provoquer des pannes majeures. Par ailleurs, un acteur pourrait cibler les systèmes de communication entre les dispositifs en réseau, empêchant la transmission des données en temps voulu et menaçant la capacité de gestion de la charge.

En 2014, la société de sécurité Symantec a découvert un important groupe de pirates informatiques (surnommé Dragonfly) qui a accédé à plusieurs reprises aux systèmes de contrôle des sociétés d'énergie. Le groupe a réussi à voler des informations à des entreprises de plusieurs pays, dont les États-Unis. Bien que Dragonfly n'ait pas encore infligé de dommages physiques à un système énergétique, il a démontré sa capacité à compromettre des dispositifs en réseau au sein du réseau intelligent.[17]

L'intégrité des données est essentielle au bon fonctionnement du secteur de l'énergie électrique, et les réseaux intelligents peuvent être davantage touchés par les problèmes d'intégrité des données en raison du niveau élevé d'automatisation. En ciblant les données de tarification et d'exploitation utilisées dans les programmes de réponse à la demande, un acteur malveillant pourrait influencer indirectement les systèmes de contrôle de la charge et

[17] Symantec, "Dragonfly: Western Energy Companies Under Sabotage Threat,".

les systèmes de réponse à la demande par les prix, provoquant ainsi la mise en marche et l'arrêt des machines côté consommateur. Par exemple, la manipulation des informations sur les prix pour faire apparaître le tarif de l'électricité comme plus chère pourrait faire en sorte que les appareils - y compris les climatiseurs, les chauffe-eau et d'autres appareils à forte consommation d'énergie - s'éteignent, alors que des prix bas pourraient les faire s'allumer.

À mesure que l'utilisation de la technologie de distribution et de transmission intelligente se développe, un nombre croissant d'appareils seront connectés aux systèmes de réponse à la demande, ce qui augmente l'impact potentiel d'une attaque. Selon la capacité d'un acteur malveillant et la sophistication d'une attaque, la manipulation des données de tarification de l'énergie pourrait toucher des millions d'appareils et des régions entières d'un pays.

2.3.1.3 L'infrastructure de comptage avancée

L'infrastructure de comptage avancée (AMI) est un dispositif conçu pour apporter une transparence et une efficacité à la consommation d'énergie dans les réseaux intelligents. Les compteurs intelligents, qui font partie de l'AMI, mesurent, stockent et transmettent des données sur la consommation d'énergie et la tension des résidences et des bâtiments commerciaux au sein d'un réseau. Contrairement aux compteurs d'énergie traditionnels, certains compteurs intelligents des systèmes AMI utilisent une technologie de communication bidirectionnelle, souvent au moyen de connexions sans fil pour envoyer et recevoir des données des services publics et des opérateurs d'énergie. Les centres de répartition et de gestion peuvent également contrôler physiquement les compteurs, avec la possibilité de connecter ou de déconnecter le courant à distance.

En plus des compteurs intelligents, l'AMI se compose d'un serveur pour recueillir, stocker et diffuser les données des compteurs intelligents et d'un système de communication pour connecter les différents composants. Ces appareils connectés aux compteurs intelligents à domicile contribuent à faciliter les programmes de réponse à la demande et d'autres programmes de consommation d'énergie. La majorité de ces appareils domestiques utilisent une infrastructure en nuage pour connecter l'appareil aux compteurs.

Les compteurs intelligents sont déjà largement utilisés par les sociétés de services publics dans les pays développés. Un rapport de Navigant Research[18] estime qu'il y avait plus de 300 millions de compteurs intelligents déployés dans le monde en 2013, et que ce nombre devrait passer à plus d'un milliard d'ici 2022.

En prenant le contrôle d'un serveur AMI, un acteur malveillant pourrait contrôler tous les aspects d'un système AMI local, par exemple bloquer ou manipuler les données sur la consommation d'énergie ou contrôler à distance d'autres fonctions. Par exemple, de nombreux compteurs intelligents sont conçus de manière à pouvoir couper à distance l'alimentation d'un bâtiment si un client ne paie pas sa facture. Ainsi, un attaquant ayant le contrôle d'un serveur AMI pourrait déconnecter à distance les compteurs, coupant ainsi l'alimentation de bâtiments ou de zones ciblés. En plus d'être en mesure d'exécuter une attaque à distance, il pourrait causer des effets physiques - le déclenchement du disjoncteur d'un bâtiment, par exemple - qui nécessiteraient une réparation manuelle sur place. De même, il pourrait également contrôler un serveur AMI pour accéder aux informations relatives à la facturation et à la consommation d'énergie, ce qui constitue un problème de confidentialité pour les consommateurs.

En 2009, des chercheurs en sécurité[19] ont démontré qu'il était possible d'installer un logiciel malveillant sur un compteur intelligent. Des simulations effectuées ont ensuite démontré la facilité avec laquelle le logiciel malveillant pouvait se propager via les serveurs AMI à des millions d'autres compteurs intelligents, ce qui leur permettait de couper à distance l'alimentation des bâtiments associés. Bien que cette attaque particulière se soit appuyée sur un défaut de conception du matériel, la facilité et l'impact de l'attaque démontrent la possibilité d'une attaque à grande échelle.

Comme pour les attaques contre les serveurs AMI, l'impact des perturbations de l'AMI sur la sécurité publique dépend de la cible et de l'ampleur de l'attaque. Une attaque ciblée pourrait avoir des répercussions locales et régionales importantes, tandis que la capacité de couper l'alimentation de millions de foyers et d'entreprises pourrait toucher un plus grand nombre de personnes, bien que les répercussions puissent être moins importantes. D'un point de vue économique, la possibilité de sous-déclarer la consommation d'énergie pourrait également

[18] Demand response refers to the ability of consumers to increase or reduce their use of electricity based on power grid needs, price changes, or special retail rates (PJM Staff White Paper).
[19] Naone, Erica, "Meters for the Smart Grid,".

entraîner des pertes financières pour les opérateurs d'énergie. Enfin, comme les compteurs seront des dispositifs physiques très visibles situés dans presque toutes les maisons, ils pourraient devenir une technologie que les gens associent comme étant représentative de toutes les technologies de la ville intelligente. Une faille de sécurité généralisée impliquant des compteurs pourrait porter un coup à la confiance du public envers toutes les technologies de la ville intelligente, technologies dont beaucoup de gens se méfient déjà.

2.3.2 Systèmes d'eau et d'eaux usées

Cette section se concentre sur les infrastructures du secteur des systèmes d'eau et d'eaux usées, dans le cadre d'une série plus large d'enquêtes sectorielles mettant l'accent sur la sécurité et la résilience. Outre les risques de sécurité générale inhérents aux réseaux d'eau, les systèmes d'eau des villes intelligentes apportent un ensemble unique de défis de sécurité, y compris les suivants :

- Difficulté de sécuriser les infrastructures physiques existantes qui sont souvent proches de leur durée de vie ou de la défaillance.
- Complexité de l'interface, de la communication et de la sécurité entre de multiples systèmes interdépendants, notamment les capteurs, les pompes, les vannes, les systèmes de contrôle, les installations de traitement, les tuyaux de distribution, les systèmes de ventilation, les systèmes de drainage.
- Emplacements isolés ou difficiles d'accès de certaines infrastructures d'eau, comme les canalisations souterraines ou les réservoirs ruraux, qui augmentent les coûts de mise à niveau, les coûts de maintenance et la dépendance vis-à-vis des moniteurs en réseau.

Trois technologies qui feront partie des futurs systèmes d'approvisionnement en eau et de traitement des eaux usées des villes intelligentes sont le traitement intelligent de l'eau, la distribution intelligente de l'eau et le stockage intelligent de l'eau.

2.3.2.1 Traitement des eaux usées

Le traitement intelligent de l'eau intègre trois processus distincts : les réservoirs d'eau, le traitement de l'eau et la distribution de l'eau. Le traitement des eaux usées intègre également trois technologies distinctes : la collecte des eaux usées, la transmission des eaux usées et les processus de traitement des eaux usées. Bien que la fonctionnalité entre l'acquisition des données et le contrôle réel soit différente, les deux processus impliquent des applications similaires. Dans les deux cas, les capteurs et les compteurs recueillent des données, la

connectivité bidirectionnelle et les réseaux de communication transmettent les données des dispositifs aux systèmes de contrôle centraux, et les automates programmables en réseau et les dispositifs SCADA automatisent les réglages du système.

De même, les systèmes de traitement des eaux usées permettent de surveiller et d'ajuster en temps réel les systèmes de collecte, les stations de pompage, ainsi que l'équilibre chimique et les conditions de traitement tout au long du processus de traitement des eaux usées. Par exemple, la technologie pourrait améliorer considérablement la viabilité des capteurs biologiques, qui utilisent des bactéries pour décomposer les matières organiques toxiques. Pour fonctionner, ces derniers doivent maintenir un système complexe de bactéries vivantes, qui ne se développent que dans certaines conditions environnementales.

Grâce à la mise en réseau et à l'automatisation des capteurs, des contrôles de température, des ventilateurs d'oxygène et d'autres dispositifs atmosphériques, les conditions atmosphériques appropriées sont maintenues pour garantir la santé du système des contacteurs biologiques rotatifs. Des installations de traitement des eaux usées compromises pourraient créer des crises de santé publique et endommager l'environnement dans les villes concernées. La perturbation de la capacité d'une ville à traiter les eaux usées pourrait provoquer des refoulements du système et pousser les eaux usées et les eaux d'égout non traitées dans les zones publiques.

Dans le pire des cas, les eaux usées pourraient refouler dans les canalisations domestiques ou dans les rues, ce qui poserait un risque important pour la santé publique. Bien qu'il soit peu probable qu'un arrêt du traitement intelligent des eaux usées endommage l'eau potable (le traitement de l'eau se fait généralement par un processus indépendant), les eaux usées non traitées dans les zones publiques pourraient exposer une population ciblée à des agents pathogènes potentiellement dangereux. Les eaux usées non traitées pourraient être expulsées dans l'environnement pendant que les installations de traitement sont réparées pour atténuer les refoulements d'égouts et éviter des risques plus importants pour la santé publique. En plus des dommages environnementaux, les eaux usées non traitées pourraient potentiellement affecter les approvisionnements en eau tout en portant préjudice aux entreprises locales et à l'économie régionale.

Un travailleur mécontent du Queensland, en Australie, a utilisé des connaissances d'initié pour accéder 46 fois aux systèmes d'une station d'épuration des eaux usées sur une période de 4

mois en 2000. L'employé a utilisé l'accès au système SCADA pour déverser plus de 200 000 gallons d'eaux usées dans des parcs, des rivières et des terrains d'hôtel, alors que l'installation n'était pas hautement mise en réseau ou automatisée[20].

2.3.2.2 Distribution de l'eau

Les systèmes de distribution d'eau intelligents remplacent ou augmentent la gestion des infrastructures existantes par des technologies automatisées et en réseau. Les vannes et les pompes sont capables de s'adapter à leur environnement, en modifiant automatiquement les vitesses et les niveaux de pression, ainsi qu'en redirigeant et en détournant l'eau selon les besoins. Ces dispositifs peuvent communiquer sans fil entre eux et avec un système de contrôle central, ce qui permet aux administrateurs de maintenir et de surveiller les fonctionnalités du système central, et d'accéder et de contrôler à distance les dispositifs de distribution.

De plus, un réseau de capteurs et de moniteurs est capable de recueillir des données sur la performance du système et la qualité de l'eau, d'alerter les administrateurs en cas d'anomalie et ainsi de mieux anticiper les pannes d'équipement avant qu'elles ne se produisent. La technologie de distribution d'eau intelligente permet d'améliorer la distribution et le mouvement de l'eau dans une ville intelligente en suivant les flux d'eau pour identifier les fuites et les ruptures de tuyaux.

Les attaques contre les systèmes intelligents de distribution d'eau pourraient avoir des conséquences régionales en matière de sécurité publique si elles coupaient l'accès à l'eau potable à certaines parties d'une ville. Les mêmes conséquences pourraient se produire si de l'eau contaminée était distribuée à un grand nombre de consommateurs, ce qui pourrait se produire en ciblant des composants critiques situés plus haut dans le système de distribution. Même si les consommateurs ou les opérateurs parvenaient à détecter rapidement les substances étrangères dans l'eau potable, il est possible qu'une certaine quantité d'eau contaminée soit consommée, avec des effets potentiellement mortels. La combinaison de ce type d'attaque et de la manipulation des capteurs de sécurité et de qualité pourrait vraisemblablement accroître les maladies et la mortalité.

[20] Abrams, Marshall, "Malicious Control System Cyber Security Attack Case Study-Maroochy Water Services, Australia."

2.3.2.3 Stockage de l'eau

Le stockage intelligent de l'eau englobe une série de technologies d'automatisation et de mise en réseau qui sont intégrées dans les réservoirs, les châteaux d'eau et autres installations de stockage, ainsi que dans les systèmes de distribution reliant ces installations à d'autres systèmes d'eau. Pour répondre à l'évolution de la demande, les systèmes SCADA et les systèmes de contrôle industriel peuvent gérer efficacement la demande et le débit d'eau. Ces systèmes surveillent également le débit entrant dans les réservoirs pour éviter les débordements et peuvent empêcher l'eau contaminée ou insalubre de pénétrer dans les réserves d'eau. Les capteurs fournissent les données en temps réel nécessaire au contrôle de ces opérations, en jaugeant constamment les niveaux, en suivant l'utilisation de l'eau et en mesurant la qualité de l'eau lorsqu'elle entre et sort des installations de stockage. Une série de capteurs permet aux opérateurs de stockage d'eau d'accéder à distance à des informations en temps réel sur les performances du système, la qualité de l'eau et la présence de substances étrangères ou dangereuses. De nombreux services d'eau, si ce n'est la plupart, pratiquent actuellement une surveillance automatisée continue des réservoirs de stockage à un certain degré.

La combinaison de l'automatisation et des systèmes SCADA dans les installations de stockage d'eau intelligentes donnera à toute personne ayant le contrôle du système un certain degré d'influence sur les ressources en eau. Un acteur malveillant pourrait contrôler à distance les composants des systèmes de stockage d'eau intelligents pour drainer l'eau stockée. En ciblant un réservoir, l'attaquant pourrait activer des vannes de décharge ou des vannes de barrage sur des réservoirs beaucoup plus grands, provoquant des inondations en aval. De même, il pourrait cibler un réservoir hydraulique ou un réservoir de stockage au niveau du sol et forcer les pompes à tirer constamment l'eau du réservoir de stockage vers d'autres parties du système.

Pendant 12 mois, entre 2012 et 2013, des hackers chinois, russes et allemands ont accédé illégalement à un système de contrôle de l'eau factice mis en place par des chercheurs américains en sécurité. Conçu pour tester les protocoles de sécurité couramment utilisés, le

faux système a subi au moins dix "attaques critiques" - c'est-à-dire des attaques qui auraient pu arrêter les véritables pompes à eau et, par conséquent, l'accès à l'eau potable[21].

Les vulnérabilités des installations de stockage d'eau pourraient constituer une menace pour la sécurité publique si elles étaient exploitées pour drainer les ressources en eau d'une ville, créer des conditions d'inondation ou entraver d'autres services essentiels. La vidange de réservoirs et de châteaux d'eau, ou la rupture de réservoirs de stockage d'eau pourraient gravement limiter la capacité d'une compagnie des eaux à répondre à la demande d'eau potable.

Même si l'eau en bouteille et d'autres sources d'eau permettraient d'atténuer certains effets, le défi logistique que représente la fourniture de sources d'eau alternatives aux citoyens d'une grande ville laisserait probablement beaucoup de personnes sans accès à l'eau. Si une attaque était menée pendant une vague de chaleur ou une sécheresse dans plusieurs installations de stockage d'eau d'une ville, il pourrait en résulter des conséquences durables dans la disponibilité de l'eau. La libération soudaine des réserves d'eau d'un réservoir, dont beaucoup peuvent contenir plus d'un million de litres d'eau, pourrait créer une surcharge d'eau, endommageant les infrastructures et les biens. Une pénurie d'eau pourrait également nuire à d'autres secteurs d'infrastructure essentiels, comme le secteur des services d'urgence, car la pression des bornes d'incendie est insuffisante et l'eau nécessaire à la production d'électricité n'est pas disponible.

2.3.3 Les transports dans les villes intelligentes

Outre les risques de sécurité généraux inhérents aux réseaux de transport, les systèmes de transport des villes intelligentes présentent un ensemble de défis en matière de sécurité, notamment les suivants :

- L'échelle et la complexité des réseaux de transport dans les grandes villes, notamment la difficulté de sécuriser la connectivité des dispositifs mobiles aux réseaux de transport et de distinguer les requêtes légitimes des dispositifs mobiles des anomalies.
- Le grand nombre de points d'accès au système, qui découle de la présence de l'informatique en réseau dans les grands systèmes, augmente le coût et la difficulté de sécuriser correctement chaque dispositif du système. Ce nombre comprend les

[21]Liebelson, Dana, "Bad News: Hackers are Coming for your Tap Water," http://www.motherjones.com/politics/2013/08/chinese-hackers-attack-trend-micro- honeypots, accessed December 3, 2014.

points d'accès câblés - dont beaucoup peuvent être situés dans des zones éloignées - et les points d'accès sans fil.

- La charge d'assurer une interface, une communication et une sécurité sans faille entre de multiples systèmes interdépendants, notamment les capteurs, les ordinateurs, les systèmes de perception des tarifs, les systèmes financiers, les systèmes d'urgence, les systèmes de ventilation, les dispositifs automatisés, les relais de puissance.
- La demande d'accès aux données en temps réel que requièrent les systèmes de transport des villes intelligentes, et les coûts associés à la maintenance et aux temps d'arrêt du service.
- Les obstacles logistiques et sécuritaires liés à l'accueil physique d'énormes volumes de passagers et de marchandises, ainsi que la réalité des failles de sécurité qui pourraient entraîner des risques pour la sécurité publique.

Les cinq technologies qui feront partie des futurs systèmes de transport des villes intelligentes sont les véhicules autonomes, le contrôle positif des trains (PTC), les systèmes de transport intelligents (ITS) et les technologies de véhicule à véhicule (V2V) et de véhicule à infrastructure (V2I).

2.3.3.1 Véhicule autonome

La technologie des véhicules autonomes permet aux automobiles de comprendre les environnements dans lesquels elles évoluent et d'exécuter des commandes sûres et efficaces sur la base de cette compréhension. Les véhicules autonomes peuvent assumer des tâches décisionnelles et opérationnelles, permettant aux conducteurs de devenir des « passagers », entièrement désengagés des exigences de la conduite. Les véhicules autonomes peuvent se diriger, sélectionner des vitesses optimales, éviter les obstacles, choisir des itinéraires efficaces, se garer eux-mêmes et avertir les passagers d'un danger imminent. La majorité des véhicules autonomes en cours de développement utilisent une architecture délibérative, ce qui signifie qu'ils sont capables de prendre des décisions entièrement basées sur la technologie embarquée - bien que beaucoup soient également capables d'incorporer des données externes lorsque cela est bénéfique. Pour recueillir les données nécessaires à leur fonctionnement, les véhicules autonomes utilisent une variété de capteurs. La technologie de détection et de télémétrie par la lumière (LIDAR) utilise des impulsions lumineuses pour identifier les marquages et les limites des voies et des routes. Les dispositifs GPS (Global Positioning System) recueillent des données géographiques spécifiques afin de faciliter le choix de l'itinéraire et la prise de décision en fonction de l'emplacement, souvent en

combinaison avec des tachymètres, des altimètres et des gyroscopes embarqués. Les caméras vidéo suivent les autres véhicules et les piétons tout en capturant des informations sur les feux de signalisation et les panneaux routiers. Les capteurs radar suivent également les autres véhicules. Les capteurs à ultrasons facilitent le stationnement en capturant des données sur les objets situés à proximité des véhicules autonomes, notamment les trottoirs et les autres voitures. Un ordinateur central embarqué traite les données provenant de ces capteurs et envoie des commandes aux systèmes de direction, d'accélération, de freinage et de signalisation de la voiture.

En 2014, deux experts en sécurité ont démontré la possibilité d'accéder et de contrôler à distance les fonctions d'un véhicule, notamment le freinage, la direction et la puissance du moteur. Bien que cette attaque ait exploité une vulnérabilité Bluetooth, les experts ont également souligné la possibilité d'utiliser les connexions cellulaires et les applications embarquées dans les véhicules comme vecteurs d'attaque supplémentaires[22].

Pour maximiser le danger pour les passagers, l'acteur malveillant pourrait également insérer subrepticement un logiciel dans l'ordinateur central d'un véhicule afin qu'il soit reprogrammé pour prendre des mesures dangereuses lorsqu'une certaine condition est remplie, par exemple lorsqu'une voiture roule à plus de 70 km par heure. Il pourrait également utiliser un logiciel malveillant pour prendre le contrôle de plusieurs véhicules simultanément, à l'insu de leurs propriétaires. Avec une masse critique de véhicules infectés, cet acteur pourrait exécuter des commandes préprogrammées pour altérer les capteurs ou exécuter des commandes dangereuses spécifiques[23].

Par ailleurs, les véhicules autonomes dépendent d'une série d'entrées externes, tels que les feux de signalisation, les panneaux de signalisation et la connaissance des autres véhicules, ce qui fait qu'une attaque sur leurs systèmes de capteurs est un moyen relativement facile et peu coûteux d'affecter un grand nombre de ces véhicules.

Bien qu'il soit difficile d'orchestrer de nombreux véhicules autonomes pour attaquer une cible spécifique, ce type d'attaque (par exemple, une collision visant un bâtiment spécifique)

9 Anderson, James et al, “Autonomous Vehicle Technology: A Guide for Policymakers,” Rand Corporation,

10 Miller, Charlie and Christopher Valasek, “A Survey of Remote Automotive Attack Surfaces. Presentation at Blackhat Conference, August 6, 2014.

pourrait réussir à provoquer une confusion de masse qui créerait des conditions de conduite dangereuses et pourrait entraîner des pertes de vies humaines. La perturbation des capteurs pour ce type d'attaque pourrait être réalisée en plaçant un dispositif de brouillage des signaux dans une zone à forte circulation (par exemple, sur un feu d'autoroute) ou en le fixant sur une voiture conventionnelle, un drone ou un autre véhicule. La tendance à la "fusion de capteurs", qui consiste à utiliser plusieurs types de capteurs, atténue certains risques en créant des redondances.

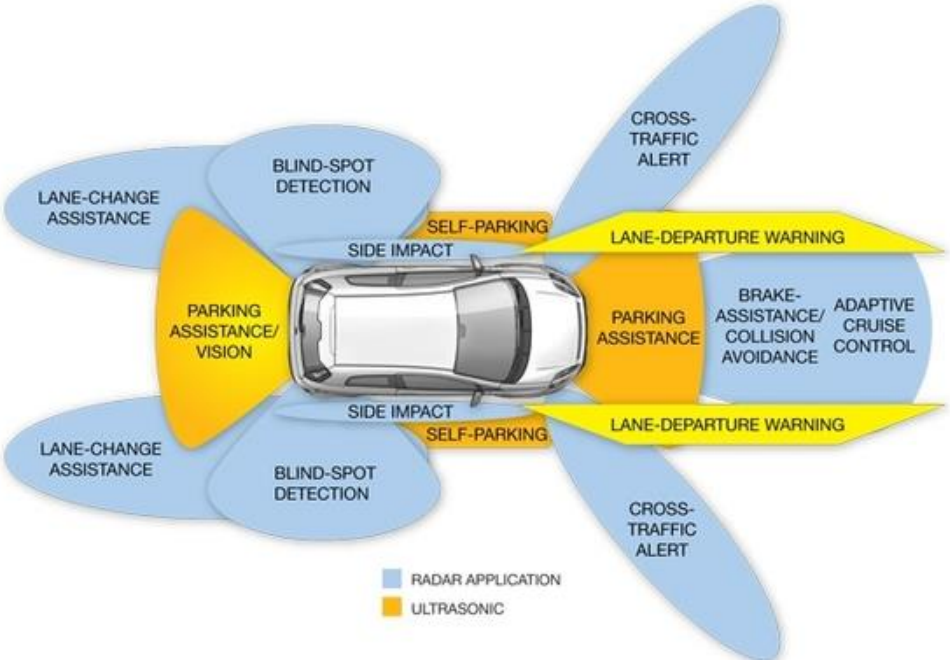


Figure 18 : Systèmes d'assistance à la conduite (tpe-voiture-autonome)

2.3.3.2 Contrôle positif des trains

Le système de contrôle positif des trains (PTC) est un système de capteurs à distance et de dispositifs de contrôle automatisés principalement conçus pour arrêter ou ralentir automatiquement un train afin de prévenir les situations dangereuses. Grâce à des connexions câblées et sans fil et à des commandes automatisées d'accélération et de décélération, le système PTC est utilisé pour prévenir les collisions entre trains, les déraillements causés par une vitesse excessive et les mouvements non autorisés des trains. Les systèmes PTC comportent généralement quatre éléments : les systèmes embarqués, les systèmes en bordure de voie, un centre de répartition central et un système de communication. Les systèmes embarqués sont situés sur les trains eux-mêmes et

comprennent le GPS et d'autres systèmes de localisation, ainsi que les systèmes de contrôle des trains. Les systèmes en bordure de voie comprennent les passages à niveau, les aiguillages et les points d'entretien. Le système de communication transmet les données de ces deux premiers systèmes au centre de répartition. Les informations sur la voie sont ensuite transmises par le centre de répartition aux trains et aux infrastructures en bordure de voie. Ces commandes peuvent donner lieu à des suggestions pour les opérateurs des trains et des infrastructures ou peuvent être programmées pour effectuer automatiquement des changements opérationnels.
Un acteur malveillant pourrait créer des conditions dangereuses en transmettant un signal de "voie libre" malgré la présence d'un train bloqué, ou en bloquant la transmission d'un signal avertissant d'un train bloqué ou de virages serrés à venir.

En 2008, un adolescent aurait accédé à distance à un système de tramway à Lodz, en Pologne, et aurait réussi à manipuler les commandes de signaux. En observant les mouvements des trains depuis des lieux publics, il a pu modifier des signaux qui ont provoqué des déraillements et des blessures[24].

De même, un acteur pourrait accéder aux systèmes PTC pour arrêter les trains à des endroits spécifiques, laissant la cargaison, les passagers et l'équipage vulnérables au détournement ou à d'autres types d'attaques. Ces cyberattaques pourraient être réalisées en envoyant des signaux défectueux directement aux composants PTC embarqués pour les avertir du danger à venir, ou en manipulant les signaux en bordure de voie (par exemple, en affichant des feux de signalisation rouges) pour arrêter les trains qui approchent. Ces deux situations pourraient déclencher des mécanismes de freinage automatique à bord d'un train ciblé. Par ailleurs, un acteur malveillant peut bloquer la disponibilité des informations sur la voie provenant d'un centre de répartition, ce qui entraîne un mode de neutralisation de la sécurité sur les trains concernés, qui se traduit souvent par un arrêt complet automatique.

En juin 2009, un train du réseau de métro de Washington DC[25] a percuté un train arrêté, faisant neuf morts et 52 blessés. La cause de l'accident a été identifiée comme étant un circuit de voie défectueux, qui n'a pas enregistré et relayé la présence du train arrêté au centre de

[24] Grant, Ian, "Schoolboy hacker derails Poland's tram network," http://www.computerweekly.com/news/2240084537/Schoolboy-hacker-derails-Polands-tram- network, accessed December 6, 2014.
[25] Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains Near Fort Totten Station.

répartition. Ne reconnaissant pas la présence d'un train à l'arrêt, le centre de répartition a indiqué que les autres trains dans le secteur devaient poursuivre leur route normalement, ce qui a provoqué l'accident.

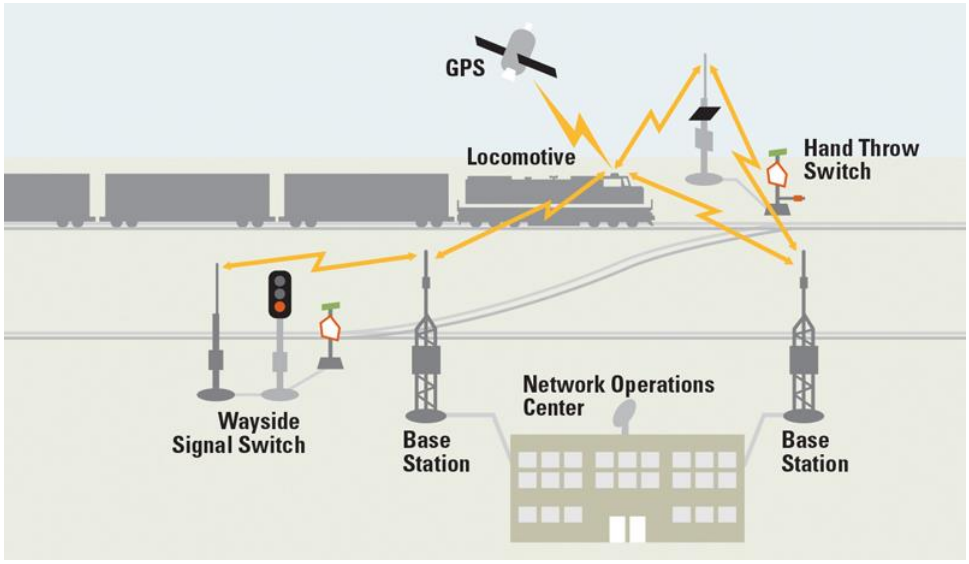


Figure 19 : Système Positive Train Control –PTC (railwayage.com)

2.3.3.3 Système de transport intelligent

Un système de transport intelligent (STI) est un dispositif dans lequel des données en temps réel sont recueillies et utilisées pour prendre des décisions automatisées concernant le fonctionnement des infrastructures et du matériel liés à la circulation. Ces systèmes comprennent généralement quatre éléments principaux : des capteurs qui recueillent des informations sur les conditions de circulation, des contrôleurs qui modifient les dispositifs de contrôle de la circulation (ex. les feux de circulation), un ordinateur central qui analyse les données et suggère des ajustements au système, et un système de communication qui relie les divers éléments. Bien que les réseaux de communication de la circulation aient traditionnellement été câblés, les villes se tournent de plus en plus vers les réseaux sans fil pour ces communications.

Par exemple, une intersection dotée de STI pourrait être équipée d'une caméra vidéo ou d'un capteur à boucle d'induction enterré pour détecter la présence de voitures. Ces capteurs transmettraient des données à un contrôleur, qui pourrait alors optimiser le fonctionnement d'un feu de circulation en fonction des conditions de circulation. Les contrôleurs peuvent être

préprogrammés pour prendre certaines mesures en fonction des données fournies par les capteurs locaux ou peuvent être commandés manuellement depuis un point central. Dans les deux cas, les données recueillies par les capteurs sont transmises à un ordinateur central, où elles sont analysées et ajoutées à l'ensemble des données recueillies.

En ciblant les communications ou les systèmes informatiques centraux, un acteur malveillant pourrait provoquer l'arrêt de plusieurs dispositifs de signalisation routière ou, plus vraisemblablement, le passage en mode de sécurité intégrée (un feu rouge clignotant). IL pourrait également cibler les dispositifs de signalisation routière eux-mêmes, provoquant ainsi des perturbations locales et régionales qui augmentent la congestion et diminuent la sécurité dans des zones cibles spécifiques.

De même, un attaquant pourrait nuire à l'intégrité des données d'un système STI en ciblant les dispositifs d'infrastructure de transport en réseau ou en insérant des informations erronées dans le système, amenant les ordinateurs centraux du système à émettre des commandes inefficaces ou involontairement dangereuses à d'autres dispositifs du réseau.

En 2014, une équipe de l'Université du Michigan[26] a accédé à un réseau de feux de circulation en utilisant du matériel facilement disponible. Une fois à l'intérieur du système, l'équipe a rapidement obtenu la capacité de modifier les feux de circulation, d'altérer les commandes logiques et de désactiver les dispositifs de signalisation. De même, les chercheurs en sécurité ont souligné la facilité d'accès aux infrastructures STI et le manque d'attention que ces vulnérabilités reçoivent à la fois de la part des fournisseurs de technologie et des administrateurs locaux.

[26] Ghena, Branden, et al, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure."; Cerrudo, Cesar, "Hacking US Traffic Control Systems.".

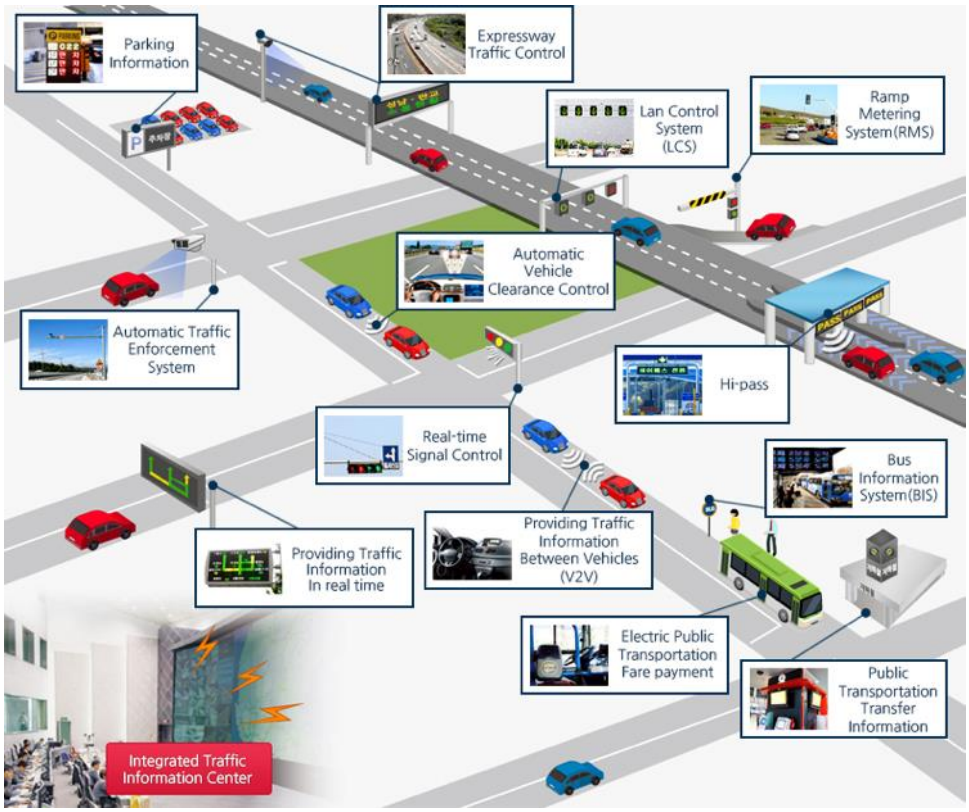


Figure 20 : Exemple de Système de Transport Intelligent -STI (peregene.com)

2.3.3.4 Véhicule-à-Véhicule et Véhicule -à-infrastructure

La technologie de véhicule à véhicule (V2V) utilise les communications dédiées à courte portée - une technologie similaire au Wi-Fi et d'une portée d'environ 1 km - pour permettre aux véhicules de "parler" entre eux et avec les infrastructures fixes telles que les bâtiments et les lampadaires. Les voitures et les camions sur un réseau V2V peuvent envoyer et recevoir des données sur leur emplacement, leur vitesse et leur distance par rapport aux autres voitures connectées afin d'alerter les conducteurs de situations potentiellement dangereuses.

Les systèmes d'aide à la circulation aux intersections aident les conducteurs à éviter les collisions dans les carrefours dangereux ou encombrés. Les systèmes de véhicule à infrastructure (V2I) permettent à l'infrastructure physique - y compris les feux de circulation et les bretelles d'accès - d'informer les véhicules de leur présence et de permettre aux véhicules d'envoyer des informations à l'infrastructure. Par exemple, un feu de signalisation pourrait suggérer une vitesse qui permettrait à un conducteur approchant d'arriver au feu lorsqu'il passe au vert, ce qui réduirait le temps d'arrêt et de départ et la congestion globale.

Un attaquant pourrait interférer avec les données relatives à la sécurité lorsqu'elles sont communiquées sur les réseaux V2V. En bloquant la sortie de données d'un véhicule concernant un freinage ou une accélération soudaine, un changement de voie ou un virage, les véhicules environnants ne pourraient pas voir ces actions. Il pourrait également manipuler le système central d'un véhicule de sorte que les données envoyées aux véhicules environnants soient basées sur des informations erronées. De même, Il pourrait perturber les réseaux de communication entre véhicules, en ciblant les dispositifs de circulation en réseau ou les points de relais de communication entre véhicules. Des informations inexactes sur les caractéristiques de la route à venir, notamment les croisements de voies, les virages serrés ou les conditions dangereuses, pourraient réduire considérablement les performances du système et affecter un grand nombre de véhicules en réseau, car les informations erronées seraient diffusées à toutes les voitures dans une zone donnée.

Les conséquences d'une attaque contre les signaux V2V et V2I pourraient affecter la sécurité publique locale dans une ville, bien que les conséquences soient probablement limitées aux accidents de la circulation et aux embouteillages. Pour manipuler les systèmes d'automatisation embarqués, un acteur malveillant devrait se tenir à proximité des véhicules cibles, ce qui limiterait la portée de l'attaque. L'attaque d'un dispositif V2I permettrait aux acteurs malveillants de toucher un grand nombre de véhicules en même temps.

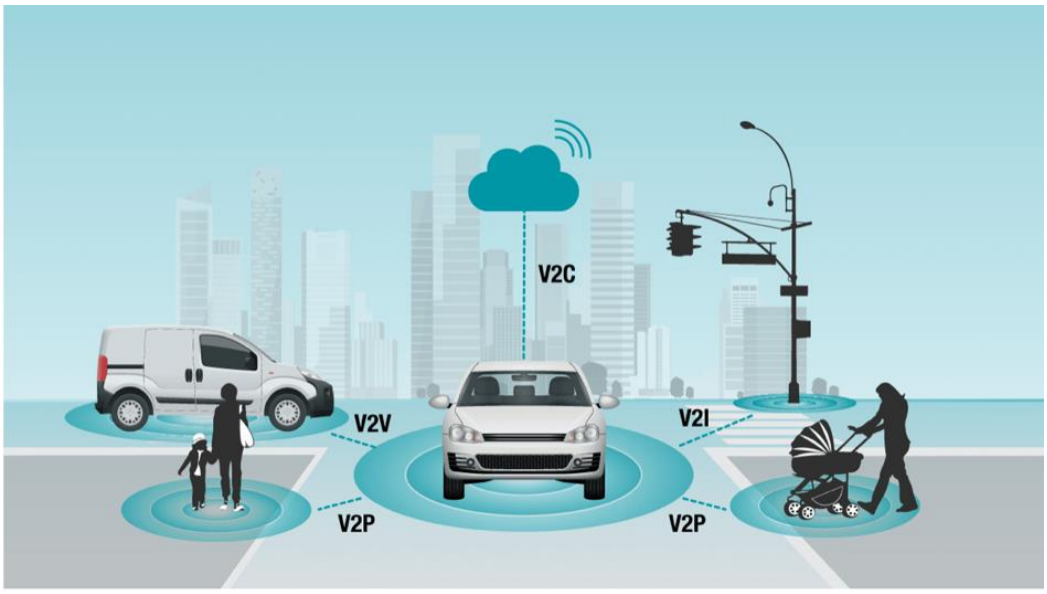


Figure 21: V2X includes vehicle-to-cloud (V2C), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P) and vehicle-to-vehicle (V2V) connectivity [e2e.ti.com]

2.3.4 Bâtiment intelligent

À mesure que les bâtiments intelligents et les systèmes d'automatisation des bâtiments deviennent plus sophistiqués, la cybersécurité devient plus importante pour les gestionnaires d'installations. Ainsi la cybersécurité fait désormais partie intégrante de leur champ d'application. S'informer sur le risque de cyberattaques et apprendre à déployer des ressources pour les prévenir doit être une priorité.

Figure 22: Les différents usages du Smart Building (adeunis.com)

C'est particulièrement vrai à la lumière des nouvelles recherches menées par la société de cybersécurité Kaspersky, qui rapporte qu'au premier semestre 2019, 37,8 % des ordinateurs utilisés pour contrôler les systèmes intelligents d'automatisation des bâtiments ont été touchés par des « cyberattaques malveillantes ». L'étude s'est penchée sur plus de 40 000 bâtiments dans le monde qui utilisent les produits de cybersécurité de Kaspersky.

Les attaques n'étaient pas spécifiquement ciblées sur les systèmes d'automatisation des bâtiments. Au contraire, la plupart étaient des logiciels malveillants trouvés sur la plupart des systèmes informatiques, mais qui ont encore affecté les ordinateurs contrôlant ces systèmes de construction intelligente. Sur les quelques 4 bâtiments attaqués sur 10, 11 pour cent ont été attaqués par des logiciels espions qui ont tenté de voler des informations d'identification de compte.

les solutions de connectivité se multiplient autour des smart building avec trois objectifs : efficacité énergétique, exploitation des opérations et confort et qualité d'usage du bâtiment. Cependant toutes ces offres ne sont pas encore bien structurées et le bâtiment 3.0, organisé autour d'un système d'exploitation central, vient tout juste de voir le jour.

Afin de mieux comprendre la complexité et la variété des technologies et acteurs qui entrent en action dans la vie des bâtiments intelligents, ci-dessous est représenté le paysage des fournisseurs de services de l'industrie des bâtiments intelligents (source Global, 2014)

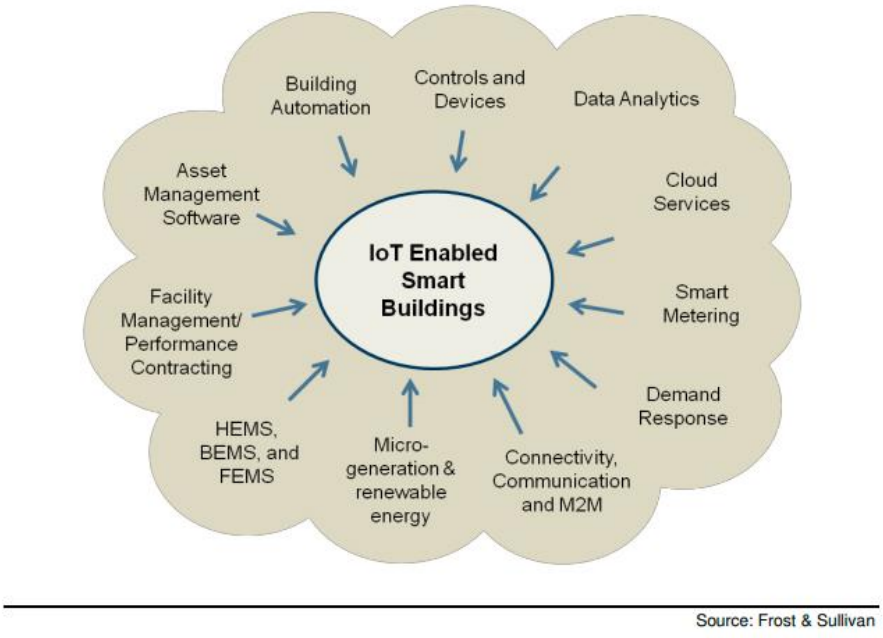


Figure 23 : Paysage des fournisseurs de services de l'industrie des bâtiments intelligents

À partir d'un environnement propriétaire de systèmes autonomes, l'industrie des bâtiments intelligents a progressivement migré vers un environnement dynamique caractérisé par des systèmes et protocoles ouverts régissant leurs aspects.

Les failles de sécurité du réseau intégré d'un bâtiment intelligent :

Les systèmes intelligents et interconnectés actuels fonctionnant sur des protocoles ouverts et avec pratiquement tous les d'autres systèmes physiques à l'intérieur du bâtiment sous leur contrôle de surveillance. L'ensemble des données en transit pour automatiser et surveiller les installations et leur fonctionnement doivent être protégé, car primordiales et parce que leur volume ne cesse de croître, assurer leur sécurité est un vrai casse-tête.

Par exemple, un réseau qui peut contrôler pratiquement tous les systèmes physiques du chauffage, la ventilation et la climatisation (CVC), l'éclairage, sécurité physique et le contrôle d'accès à la gestion de l'énergie et à l'agrégation des données a le potentiel de déclencher des compromis de sécurité à grande échelle pour tous ces systèmes. Des attaquants qui réussissent l'infiltration du réseau peuvent potentiellement infiltrer l'entreprise.

Toutefois, l'ampleur des dommages peut gonfler considérablement lorsque ces systèmes ouverts sont superposés à l'IoT, qui emprisonne essentiellement la connexion de tous les systèmes et services de construction tels que la surveillance, l'analyse avec une superposition d'un réseau de protocole Internet (IP) qui élimine toute intervention humaine.

Les activités centrées sur l'IoT offrent des avantages de plus en plus uniques et de nouveaux défis. Les avantages incluent l'accès en temps réel, la vaste génération, l'analyse de données et l'interconnectivité des systèmes et les appareils. Toutefois, ces avantages offrent peu de valeur à moins que la décision cruciale de partager les données et les réseaux soit prise simultanément, permettant ainsi l'accès à plusieurs fournisseurs de services pour puiser dans les différents systèmes et dispositifs d'un bâtiment intelligent.

Cet accès implique des failles de sécurité potentielles qui pourraient rendre un bâtiment intelligent, ses occupants et fournisseurs de services impuissants face aux actions dommageables d'un adversaire contre les réseaux corrompus, et causer des pertes opérationnelles et financières importantes.

Avec l'IoT, 2 larges seaux d'éléments sont menacés en cas de cyber-violation (machine et données), dans l'exposition.

Premièrement, par définition, l'élimination de l'intervention humaine dans le domaine de l'IoT implique un environnement M2M à l'intérieur du bâtiment qui englobe tous les systèmes physiques qui peuvent interconnexion et intercommunication par l'intermédiaire d'un réseau IP qui est en jeu en cas de cyber-violation.

Deuxièmement, la relation inséparable de l'appareil et des données réunies dans le cloud ou localement peuvent être compromises en cas de cyber-violation.

Ces deux larges seaux de machines, les données et leurs inter-connexes intrinsèques peuvent entraîner des dommages cumulatifs dans toutes les couches du portefeuille d'entreprises, de bâtiments et d'installations.

2.3.5 La santé intelligente

Les cybermenaces sont le principal risque pour les organisations de soins de santé. La santé est l'un des deux principaux secteurs les plus ciblés par les cybermenaces. En 2019, les rançongiciels ont augmenté de 118%, tandis qu'au cours des deux dernières années, 90% des établissements de santé ont subi une sorte de cyberattaque. Le risque de cyberattaque est une préoccupation croissante en raison de la croissance incroyable du nombre et les types de dispositifs médicaux qui composent l'Internet des objets médicaux (IoMT). Ces produits médicaux intelligents comprennent les appareils portables, les appareils mobiles, les applications, les capteurs, robotique, moniteurs, équipement médical, implants et bien d'autres, et ils comprennent un marché mondial qui devrait dépasser 410 milliards de dollars d'ici 2020. Les appareils IoMT et les systèmes manquent souvent de contrôles de sécurité, ce qui signifie qu'ils créent de façon exponentielle plus d'opportunités que les cybercriminels peuvent exploiter.

Un autre facteur de risque de cyberattaque est que les organisations de soins de santé évoluent leurs modèles de prestation de soins et l'adoption de nouvelles technologies par rapport à leur risque. Par exemple, de nombreuses organisations sont en train de quitter les soins segmentés en soins basés sur la valeur ou en milieu communautaire, ce qui se traduit par un flux de données interconnectées tout au long du cycle de vie du patient via l'interopérabilité entre les appareils et les données, augmentant la complexité de l'écosystème. En conséquence, la surface d'attaque est beaucoup plus étendue et difficile à protéger, car le périmètre de sécurité comprend une empreinte numérique largement étendue, y compris plusieurs organisations, appareils IoMT et tiers.

Et, malgré plus de surveillance réglementaire et des investissements de sécurité accrus, les violations continuent de se produire en raison du manque d'hygiène de sécurité dans de

nombreuses organisations “ même si les organisations faisaient des efforts de transformation numérique, leurs pratiques de gestion des risques ne suivent toujours le rythme”.

Les actifs considérés comme critiques au sein d’un système de santé sont :

- Les systèmes d'information sanitaire, c'est-à-dire les réseaux d'information dans les hôpitaux.
- Les référentiels de données cliniques, c'est-à-dire les bases de données de chaque hôpital où les informations sont stockées localement.
- Les serveurs d'authentification, c'est-à-dire pour effectuer le contrôle d'accès et l'authentification des utilisateurs.
- Le système d'information de laboratoire (LIS) - Systèmes d'information radiologique (RIS).
- Les systèmes d'archivage et de communication d'images (PACS), c'est-à-dire le transfert des résultats de radiologie.
- Les composantes du dossier de santé électronique ;
- Le service de dossier de santé du patient.
- Le service de prescription électronique.

La sécurité informatique dans les systèmes, services et applications de santé est positionnée comme une préoccupation majeure en raison de la confidentialité élevée et les exigences de confidentialité des données de santé sensibles. La cyber santé est confrontée à de nombreux défis en matière de sécurité.

D'après une étude menée par l’ENISA portant sur différentes structures de santé européenne, les répondants ont été interrogés sur les défis de cybersécurité les plus importants.

Les résultats sont illustrés ci-dessous :

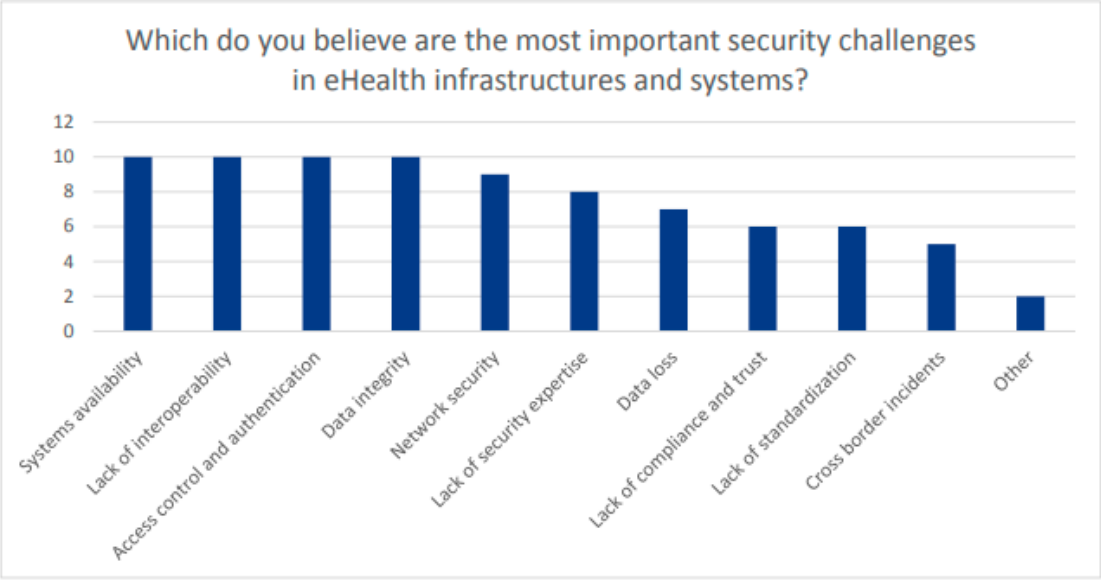


Figure 24: Les défis majeurs de la sécurité de la santé numérique - ENISA

3 DE LA SMART CITY A UNE VILLE SECURISEE

Actuellement, la stratégie adoptée pour protéger les villes intelligentes comprend principalement des solutions d'atténuation traditionnelles, principalement techniques, telles que le chiffrement, le contrôle d'accès, les normes de l'industrie et les protocoles, les systèmes de remédiation informatiques et la formation des employés. Compte tenu de l'importance cruciale de la technologie et de l'infrastructure des villes intelligentes pour la vie urbaine, bien que cela ait déjà eu un impact, les experts en sécurité s'accordent à dire que la protection de ces systèmes nécessite des interventions systémiques plus vastes, y compris des mesures d'atténuation (réduction de l'intensité ou de la survenance des incidents) et préventives (pour prévenir les accidents ou les occurrences) et pour assurer la mise en œuvre par le biais de plans et de réglementations axés sur le marché et d'applications axées sur la gouvernance.

3.1 SOLUTIONS D'ATTENUATION CONVENTIONNELLES

Comme nous l'avons vu précédemment, les dispositifs des villes intelligentes présentent généralement de vastes surfaces d'attaque qui exposent les dispositifs à un certain nombre de failles potentielles, en particulier dans les systèmes de contrôle qui contiennent des composants utilisant des systèmes vétustes qui sont rarement mise à jour.

La méthode actuelle de protection des systèmes consiste à utiliser une série de solutions techniques et de méthodes de sécurité empiriques bien connues pour tenter d'empêcher l'accès et permettre la récupération en cas de dommage ou en cas de compromission. Par exemple, l'utilisation de contrôle d'accès (double facteur, identification par biométrique), de pare-feu pour cloisonner les réseaux entre eux, des mécanismes de chiffrement de bout à bout, de procédures garantissant l'application régulière de correctifs logiciels et la capacité de répondre par des mises à jour urgentes pour éliminer les vulnérabilités au fur et à mesure qu'ils se produisent, de pistes d'audit de l'utilisation et des journaux des modifications, ainsi que de sauvegardes hors site efficaces et de plans de récupération d'urgence.

Le but de l'utilisation de ces mécanismes est de minimiser la surface d'attaque et de rendre le système et l'infrastructure résilients et récupérables en cas de panne majeure. Par conséquent, pour les systèmes critiques, il doit avoir une redondance intégrée pour garantir

que le système auxiliaire puisse prendre automatiquement le relais en cas de panne du système principal.

La solution peut inclure l'utilisation de solutions décentralisées basées sur le cloud (où les données et les calculs sont localisés sur plusieurs sites) ou de solutions techniques totalement indépendantes. Bien qu'il s'agisse d'une solution optimale, il est également vrai que la création d'une véritable redondance est souvent difficile et coûteuse. De plus, dans un système distribué complexe avec de nombreux composants, ces solutions doivent être les mêmes dans tout le système, car la solidité de l'infrastructure ou de l'entreprise dépend du maillon le plus faible. De plus, il arrive souvent que ces types de solutions soient ajoutées après le développement du système, plutôt que d'être incorporées dans la conception.

Ces solutions techniques sont souvent renforcées par un personnel dédié qui supervise la maintenance de ces systèmes, notamment en surveillant les problèmes de sécurité et en répondant rapidement aux anomalies ou à une attaque informatique.

En outre, les employés non informatiques de l'organisation peuvent recevoir une formation sur les bonnes pratiques de sécurité, telles que les mots de passe plus forts, les mises à jour logicielles, la sécurisation de fichiers et les attaques de phishing. Cependant, la formation n'est souvent dispensée qu'une seule fois et le respect des bonnes pratiques par le personnel n'est pas contrôlé.

Si ces mesures de sécurité ont une réelle utilité, elles ne constituent toujours pas une solution complète, d'autant plus que les technologies intelligentes évoluent rapidement et deviennent de plus en plus indispensables au fonctionnement des villes. Il conviendrait plutôt d'adopter une approche plus systématique, à la fois en termes de conception technique et de formation. L'approche de sécurité proactive et préventive, plutôt que réactive et corrective, devrait être utilisée par municipalités pour la gestion urbaine et la fourniture d'infrastructures. La sécurité dès la conception vise à renforcer la sécurité des systèmes dès le départ au lieu d'essayer de les superposer après le développement.

L'évaluation des risques de sécurité doit être un élément fondamental du processus de conception et tous les aspects des systèmes de sécurité doivent être rigoureusement testés avant que le produit ne soit vendu, y compris une phase pilote dans un environnement de post-production qui comprend des tests de sécurité d'un produit lorsqu'il est déployé dans des contextes réels et qu'il fonctionne dans le cadre d'un réseau plus large de technologies.

Il s'agit également de mettre en place un engagement permanent en matière de cybersécurité, notamment un mécanisme de suivi des produits tout au long de leur cycle de vie, un processus de soutien et de correction au fil de l'eau, et une procédure de notification aux clients lorsque des risques de sécurité sont identifiés.

En ce qui concerne l'infrastructure de contrôle et les systèmes logiciels de la ville, les fournisseurs devraient être tenus de fournir une documentation et des procédures de sécurité, et d'en effectuer un audit de sécurité complet afin d'identifier les points fragilités, d'entreprendre des correctifs de sécurité et de mettre à niveau les futurs accords de niveau de service en matière de sécurité. Si les systèmes ne peuvent pas être corrigés et qu'il subsiste des failles permanentes susceptibles de fragiliser les systèmes critiques, des plans de remédiation fermes doivent être mis en place pour les mettre à niveau ou les remplacer.

En ce qui concerne la surveillance des aspects sécuritaires des technologies de la ville intelligente, nous recommandons la formation d'une équipe de sécurité au sein des municipalités, dotée de compétences et de responsabilités particulières allant au-delà de l'administration informatique quotidienne. La municipalité constitue également une équipe d'intervention en cas d'urgence informatique de la ville pour s'attaquer activement à tout incident de sécurité en cours. Dans le cadre de son travail quotidien, l'équipe centrale de sécurité devrait consulter les fournisseurs de cybersécurité pour se tenir au courant des vulnérabilités potentielles et des contre-mesures applicables. En outre, l'équipe devrait créer un canal formel avec les industriels et les équipementiers pour le retour d'information sur le niveau de sécurité réel des composants et des technologies déployées.

Un changement radical dans l'éducation et la formation en matière de sécurité est indispensable pour toutes les personnes impliquées dans les projets de villes intelligentes. Ainsi, au sein des collectivités, des fournisseurs d'infrastructures et de services publics, une formation avancée à la sécurité devrait être développée, mais surtout pour le personnel impliqué dans la conception, l'acquisition, le déploiement et le fonctionnement quotidien des technologies urbaines.

C'est important, car, même si un système peut disposer d'un ensemble de solutions de sécurité technique robustes, celles-ci peuvent être annulées par des failles de sécurité ou tout simplement des erreurs humaines.

De même, des programmes de ce type devraient être mis en place pour les développeurs et les industriels afin de souligner la nécessité d'une approche de la sécurité dès la conception, en particulier pour les jeunes entreprises et les PME qui ne disposent pas toujours des compétences internes en matière de sécurité. De plus, la formation doit faire partie d'un programme continu de développement professionnel afin de maintenir les compétences en la matière et de se tenir informée des nouvelles technologies et dernières menaces.

3.2 INTEGRATION ET MISE EN APPLICATION

C'est une chose de préconiser des mesures d'atténuation plus strictes, mais c'en est une autre de veiller à ce qu'une approche plus systémique de la cybersécurité pour les villes intelligentes soit largement mise en œuvre et appliquée.

Il est donc nécessaire de réfléchir aux dispositifs les plus adaptés pour encourager la participation du secteur public et du secteur commercial et pour pénaliser ceux qui ne parviennent pas à améliorer la sécurité de leurs produits, systèmes et services.
En général, il existe deux voies pour améliorer les mesures d'atténuation :

- L’adoption par le marché.
- La réglementation et l'application de la loi par les gouvernements.

L'approche dirigée par le marché consiste à ce que les fournisseurs développant des technologies pour les villes intelligentes adoptent une position proactive et autorégulatrice en matière de sécurité. Dans ce cas, les éditeurs de logiciels choisissent d'adopter la sécurité dès la conception comme norme de base, de collaborer entre eux pour créer des normes efficaces à l'échelle du secteur et d'établir de meilleures pratiques.
Ce faisant, la sécurité devient une norme attendue et l'adoption d'une approche vertueuse de la sécurité par les entreprises leur procure un avantage concurrentiel sur celles qui ne s'y conforment pas. L'approche orientée marché est censée être en partie motivée par la concurrence, crainte des atteintes à la réputation et des litiges causés par un incident majeur en matière de sécurité, et les avantages de l'autorégulation, au lieu d'une méthode d'application par le biais de sanctions et d'amendes.

Bien qu'il existe actuellement une approche de la sécurité guidée par le marché, elle adopte principalement l'approche d'atténuation faible décrite ci-dessus et non la sécurité par la conception. Cela s'explique en partie par le fait qu'il n'y a actuellement que peu de pression sur la sécurité par les collectivités et les acheteurs, principalement en raison d'une mauvaise compréhension des vulnérabilités de sécurité et de leurs conséquences potentielles, ainsi que des pratiques d'achat non adaptées. En outre, les impératifs de mise sur le marché des produits le plus rapidement possible et la réalisation de bénéfices rapide rogne souvent sur les mécanismes de protection et de sécurité.

Ainsi, les réponses axées sur le marché devraient s'accompagner d'une réglementation plus "forte" et de meilleures pratiques de gestion de la part des municipalités et des opérateurs d'infrastructures. L'approche fondée sur la réglementation vise à encourager le déploiement de technologies sécurisées par des mesures de conformité et une surveillance active des solutions développées.La première approche nécessite l'élaboration de normes, de directives et de meilleures pratiques en matière de sécurité auxquelles les déploiements des villes doivent se conformer sous peine d'encourir une certaine forme de sanction, comme des poursuites, des amendes ou la perte d'un contrat. De nombreuses initiatives de normalisation sont en cours - par des organismes tels que l'Organisation internationale de normalisation, l'Institut britannique de normalisation, l'Institut national américain de normalisation - afin de définir des spécifications minimales pour le développement technique et le déploiement des technologies. Ce dernier point nécessiterait la mise en place de structures et de procédures de gestion pour garantir le respect et l'application de la conformité.

Par exemple, les municipalités devraient instituer un comité de maitrise des risques qui identifieraient les menaces et surveilleraient les vulnérabilités potentielles et superviseraient la stratégie d'atténuation des risques. Ces comités pourraient bénéficier d'un sous-comité spécifiquement axé sur la sécurité des logiciels, des infrastructures et des réseaux communications. Ce sous-comité devrait superviser et vérifier le travail de l'équipe de sécurité interne, donner des conseils sur les priorités et le programme de sécurisation, s'assurer que des plans et des processus de réponse et d'atténuation sont en place, et s'assurer qu'il existe une communication claire à destination du public. Son rôle serait également de certifier que les technologies et logiciels sont conformes aux exigences légales et réglementaires.

De même, les municipalités devraient intégrer la sécurité dès la conception et la maintenance continue de la sécurité (y compris l'application de correctifs dans les délais et la réponse aux incidents 24 heures sur 24 et 7 jours sur 7) dans leur processus d'achat et leurs contrats de niveau de services.

Ils devraient également souscrire à des offres de surveillance continue de leurs logiciels et infrastructures urbaines telles que les programmes de Bug Bounty. Ces programmes permettent aux développeurs de découvrir et de corriger des bogues avant que les personnes malveillantes et le grand public en soient informés, évitant ainsi des abus.

À l'occasion de cette étude, nous n'avons pas trouvé d'exemple concret d'une municipalité qui, à l'heure actuelle, met en place une telle surveillance systémique et renforcée de la sécurité ou des processus achats au-delà de la recherche de stratégies d'atténuation existantes. Cela est dû en grande partie à un manque de connaissances et de compétences approfondies, ainsi qu'à l'inertie institutionnelle. Par conséquent, les technologies urbaines ont été par le passé, et sont encore aujourd'hui, achetées en tenant peu compte de manière coordonnée des risques. Compte tenu des préjudices potentiels et des coûts associés, il convient de mettre fin à cette approche fragmentaire et improvisée et de la remplacer par une approche plus systémique et coordonnée de la sécurité.

3.3 VERS UNE APPROCHE PREVENTIVE

Même avec une stratégie d'atténuation solide et des procédures d'application efficaces, il n'est pas possible d'éradiquer toutes les vulnérabilités de sécurité et les risques associés à la ville intelligente. Il y a donc lieu d'envisager une approche préventive, qui consiste à construire des infrastructures urbaines délibérément "*air-gapped*" (non mis en réseau et accessibles à distance) et "autonome" (c'est-à-dire non automatisés par code), ce qui permettrait d'éviter de nombreux problèmes de sécurité logicielle.

Une telle approche prudente, qui remet les logiques commerciales et les flux de profits de nombreux vendeurs de matériel et développeurs de logiciels, sera qualifiée de "rétrograde" par une grande majorité des acteurs des villes intelligentes. Toutefois, à l'heure actuelle, préconiser une approche préventive serait considéré comme un moyen radical de sécuriser les infrastructures urbaines, car cela nécessite de recadrer la valeur autour de la technologie et de repenser l'équilibre entre efficacité et sécurité. Il s'agit d'un plaidoyer pour les

composants et systèmes électromécaniques conventionnels qui fonctionnent de manière fiable sans surveillance logicielle supplémentaire ni accès au réseau.

Le fait de devoir envoyer une personne physiquement auprès d'un composant pour le réactiver, reconfigurer les paramètres ou le réparer peut sembler coûteux et fastidieux alors que cela pourrait être fait à distance. En effet, à l'ère de la connectivité omniprésente, de l'informatique en nuage, des systèmes intégrés et interopérables et du contrôle à distance, l'idée d'avoir une ségrégation physique dans les systèmes critiques peut sembler contre-intuitive. Pourtant, il peut s'agir d'une méthode de sécurité efficace contre les pirates informatiques, les effets en cascade en cas d'attaques, et réduit considérablement les vulnérabilités.

Actuellement, la mise en œuvre de mesures préventives sera difficile à promouvoir et à promulguer étant donné l'adoption généralisée des discours technophiles de "*progrès*" mis en avant par l'urbanisme intelligent. C'est particulièrement le cas dans le climat actuel qui encourage les villes à former des partenariats public-privé avec des entreprises et à externaliser ou privatiser des services, et où l'accès aux subventions gouvernementales sera difficile sans prétendre créer et mettre en œuvre des solutions innovantes et de pointe en matière de ville intelligente. Cette situation pourrait toutefois changer avec l'augmentation des attaques informatiques à l'encontre des infrastructures et des systèmes des municipalités. Fort de toutes ces analyses, certaines recommandations à l'égard des collectivités locales semblent pertinentes en vue d'un développement plus sécurisé de la ville intelligente.

Les villes doivent être force de proposition envers les constructeurs en exprimant clairement leur besoin en termes de cybersécurité afin que ceux-ci l'intègrent dès le début de leur cycle de développement. On pense alors à l'application de la méthodologie EBIOS dans l'analyse de risque inhérent à la sécurisation des villes intelligentes, à la définition d'une véritable politique et d'une charte de sécurité établie par la ville à destination de l'ensemble des acteurs de la ville.

De véritables campagnes de sensibilisation des citoyens à la cybersécurité par les villes elles-mêmes (bandeaux publicitaires, affichage public …) doivent être mises à l'ordre du jour.

Les villes doivent inclure cette gouvernance de la cybersécurité dans leur organisation en créant des fonctions dédiées à l'instar des RSSI (Responsable de sécurité des systèmes d'information) dans les organismes publics ou privés, définir les politiques de sécurité, piloter les analyses de risques et coordonner les responsables de la sécurité des parties prenantes.

Les villes doivent également développer la notion de « framework » de cybersécurité, de façon à l'intégrer à tous les stades du déploiement d'une ville intelligente, de permettre à l'ensemble des acteurs d'avoir un standard et des normes à respecter dans l'implémentation de leurs solutions, de décrire les méthodes de management du risque à mettre en œuvre. À terme il deviendra le guide indispensable pour les municipalités désirant mettre en œuvre de tel projet.

Un axe important à développer sera également de réfléchir à des moyens de partager les différentes expériences et implémentations des smart city à l'échelle nationale d'abord puis à l''international et ainsi favoriser la mise en place de normes et standards communs.

Enfin, il est nécessaire d'associer à la construction des villes intelligentes les citoyens pour les sensibiliser aux bonnes pratiques de la sécurité. En effet les moyens de communication du citoyen peuvent constituer le maillon faible dans la chaine sécuritaire. De même que les organismes publics ou privés ont élaboré pour leurs employés une « charte utilisateur des TIC », les municipalités doivent sensibiliser leurs citoyens aux risques encourus lors du vol ou du piratage de leur moyen de communication. Certaines grandes villes, comme Los Angeles ou Barcelone ont déjà commencé cette sensibilisation grâce à des bandeaux affichés lors de l'utilisation des applications mobiles de la ville ou de leur portail. Le message politique associé, s'il ne doit pas être anxiogène, doit cependant montrer l'intérêt prioritaire que porte la municipalité à la sécurité de ces citoyens et de leurs données.

3.4 VERS UNE VILLE SURE ET RESILIENTE

La mise en œuvre de la sécurité et de la résilience des villes intelligentes est complexe et devrait faire partie d'une planification préalable de la part des dirigeants. C'est pourquoi nous Une feuille de route pour la sécurité et la résilience intègre la vision et les valeurs de l'initiative globale de la ville intelligente et détermine les objectifs, les stratégies et les actions qui garantissent la sécurité, la résilience et la protection des données sur le territoire, et établit des structures et des processus pour une collaboration et une coordination solide dans la gouvernance. La feuille de route aborde en outre les obstacles potentiels et détermine les étapes à franchir pour suivre et communiquer les progrès réalisés au cours de la mise en œuvre.

Les villes varient en termes de taille, d'organisation, de culture et de style de gouvernance. Indépendamment de la structure globale d'une ville, les éléments clés d'une feuille de route devraient inclure les 7 étapes suivantes :

1 : Définir une vision de la ville intelligente :

Une feuille de route s'appuie sur la vision exposée dans la stratégie de la ville intelligente concernée. La vision encadre le développement de la feuille de route (par exemple, pourquoi une ville veut-elle devenir une ville intelligente ? Quels sont les objectifs et les principes sous-jacents du développement de la ville intelligente ?)

2 : Assurer une large participation des parties prenantes

Identifier et faire participer les principales parties prenantes tout au long du développement et de l'exploitation de la ville intelligente.

3 : cartographie les risques critiques et les interdépendances

Le plan de développement de la ville intelligente doit identifier les secteurs critiques (par exemple, l'énergie, les transports). Pour obtenir une vue d'ensemble du paysage des risques de la ville intelligente, décrivez ces domaines et les interdépendances fonctionnelles et techniques connexes qui peuvent avoir des effets en cascade et présenter des caractéristiques systémiques. Identifier et évaluer les changements et les conséquences possibles que l'utilisation des TIC intelligentes entraîne pour la prestation de services, les opérations et la gouvernance liées à la sécurité et à la résilience de ces domaines et des infrastructures et organisations connexes.

4 : Atténuer les risques et garantir la réalisation des avantages

Décrire les stratégies de gestion du risque en tenant compte des coûts d'investissement et d'atténuation ainsi que des répercussions sur la convivialité par rapport aux avantages attendus. Décrivez les mesures d'atténuation relatives aux processus, à la technologie et aux personnes.

5 : Définir des niveaux adéquats de sécurité et de résilience :

La sécurité n'est jamais absolue. Fixez des objectifs en matière de sécurité, de résilience et de protection des données et comparez-les à la posture actuelle de la ville. Élaborez des mesures pour combler les lacunes, en vous appuyant sur les normes et les meilleures pratiques internationales.

6 : Adapter les structures de gouvernance :

Mettre en place des incitations pour favoriser la collaboration et la coordination dans toutes les questions liées à la sécurité et à la résilience. Concevoir des structures et des mesures de gouvernance agiles et réactives pour renforcer la transparence, la participation, la responsabilité et le leadership.

7 : Garantir des décisions d'investissement éclairées :

Les investissements doivent être fondés sur une évaluation solide des risques et une gestion des avantages. La décision d'investissement - et sa prise en compte dans le processus budgétaire - doit également tenir compte des coûts liés aux implications en matière de sécurité et de confidentialité, des mesures d'atténuation des risques et de l'intégration dans l'architecture globale de sécurité de l'information de la ville. Pour profiter des avantages attendus, une ville doit avoir les capacités nécessaires (par exemple, la compétence, la capacité et la capacité) pour réaliser la valeur du

déploiement de la technologie intelligente. Ces capacités correspondent étroitement à la maturité globale de la ville en matière de technologies intelligentes.

4 CONCLUSION

Ces villes fonctionnent grâce à de nouvelles technologies, de nouveaux systèmes et des réseaux complexes conçus pour superviser et fournir des services au public, aux entreprises locales et aux pouvoirs publics. Ces environnements qui interconnectent le physique et le numérique sont susceptibles de présenter un fonctionnement imprévu et de nouveaux risques. Les villes investissent dans ces nouvelles technologies, en espérant un retour sur investissement. Pourtant, le risque de ces technologies doit être géré et les avantages doivent être suivis pour garantir leur réalisation. Ces deux aspects représentent un défi important, car ils se manifestent à différents endroits, notamment dans la technologie elle-même, mais aussi dans les processus, les politiques, les lois et, en particulier, les citoyens.

Elles exigent un apprentissage et une innovation constantes. La maturité nécessaire au déploiement de la technologie et à la gestion des risques jouera un rôle important dans l'équilibre bénéfice-risque. La taille et la densité d'une ville, son environnement, son histoire, ses perspectives d'avenirs influenceront ce calcul, tout comme son intégration dans les structures nationales ou régionales plus larges, ainsi que les cadres politiques et juridiques.

Il est également important de reconnaître les limites des promesses de la technologie pour l'avenir de l'infrastructure urbaine.

Ainsi, il est essentiel qu'une collaboration ait lieu entre les fournisseurs, les fabricants d'appareils et les gouvernements pour élaborer une réglementation plus stricte en matière de sécurité des technologies intelligentes. Les organisations et les industriels doivent adopter de nouvelles normes et directives pour s'assurer que les systèmes soient « sécurisés par conception » et effectuer des essais avant et après l'installation pour remédier à tout défaut. En outre, les opérateurs des villes intelligents doivent chercher à comprendre bien en amont les problèmes de sécurité auxquels sont confrontés leurs environnements et systèmes s'ils veulent atténuer les risques avant que les incidents ne se produisent. Ce n'est qu'en gardant une longueur d'avance que les municipalités pourront pleinement profiter des avantages, prévenir les défaillances techniques et se défendre contre la cybercriminalité.

Les villes intelligentes doivent jongler entre différents enjeux pour assurer d'être une ville dite « intelligente et sûre ».

Les enjeux de souveraineté et juridique permettre de légiférer sur la manière de gérer les données afin de garantir leur utilisation dans de bonnes conditions. Le RGPD est devenu par conséquent la clé de voute de l'arsenal législatif actuel. Mais le statut juridique des données reste difficile à déterminer.

Enfin en termes de résilience, pour les villes comme pour les organisations, la capacité à assurer la continuité des services pour la ville et les citoyens en cas de catastrophe, à se reconstruire rapidement et à prospérer après l'événement est devenue une notion vitale.

La cyber-résilience va encore plus loin en veillant à ce que les systèmes TIC continuent de fournir des services en cas de sinistre majeur.

La ville intelligente est une démonstration de la gouvernance moderne, et c'est aussi un sens de développement socio-économique et technologique inévitable. Cependant, comment équilibrer la relation de droits entre la société et la population tout en améliorant les capacités de gouvernance et en protégeant les intérêts publics, c'est un test majeur sous de multiples perspectives technologiques, juridiques, morales et éthiques.

En définitive, la responsabilité de la mise en œuvre des ville intelligentes incombera aux maires. Pourtant, l'expérience pratique de la gestion de systèmes aussi vastes et complexes est rare. La coopération et la collaboration entre les villes et les États s'avéreront essentielles pour le bon fonctionnement des villes intelligentes, ainsi que pour l'acceptation et la confiance du citoyen dans la vision de la ville intelligente.

SOURCES

- https://www.lefigaro.fr/secteur/high-tech/aux-etats-unis-22-villes-ont-deja-ete-attaquees-par-des-pirates-informatiques-en-2019-20190715
- https://www.usine-digitale.fr/article/la-nouvelle-orleans-en-etat-d-urgence-face-a-une-cyberattaque-d-envergure.N913859
- https://www.ipcc.ch/languages-2/francais
- https://www.un.org/sustainabledevelopment/fr/development-agenda/
- https://unfccc.int/fr/process-and-meetings/l-accord-de-paris/qu-est-ce-que-l-accord-de-paris
- https://architexturez.net/pst/az-cf-169297-1435054977]
- https://news.un.org/fr/story/2018/05/1014202
- https://wedocs.unep.org/bitstream/handle/20.500.11822/30798/EGR19ESFR.pdf
- https://unhabitat.org/sites/default/files/2020/05/hsp_ha_1_4_f.pdf
- https://fr.techtribune.net/iot-nouvelles/marche-du-transport-intelligent-dune-valeur-de-1565-milliards-de-dollars-dici-2025/13828/
- https://www.smrt.com.sg/Portals/0/SMRT_OpsReview2020_Full_16042021.pdf
- https://www.chinadiscovery.com/shanghai/shanghai-metro.html
- http://www.urbanrail.net/as/id/jaka/jakarta.htm
- https://www.itdp.org
- https://www.velib-metropole.fr/service
- https://unece.org/DAM/hlm/documents/Publications/U4SSC_Deliverable-Connecting-Cities-and-Communities.pdf https://nyc.streetsblog.org/wp-content/uploads/2018/01/TSTC_A_Way_Forward_CPreport_1.4.18_medium.pdf
- https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/07/2020-autonomous-vehicles-readiness-index.pdf
- https://www.iea.org/
- https://www.energyst.com/fr-be/actualites/micro-reseaux/
- https://fr.wikipedia.org/wiki/Stockage_de_l%27%C3%A9nergie
- https://www.centrales-next.fr/glossaire-energies-renouvelables/centrale-virtuelle/
- https://www.smartgrids-cre.fr/introduction-aux-smart-grids
- https://www.smartgrids-cre.fr/projets/avenir
- https://www.smartgrids-cre.fr/projets/nice-grid
- https://arena.gov.au/projects/?project-value-start=0&project-value-end=200000000
- https://www.smartgrids-cre.fr/projets/ielectrix

- https://www.globaltimes.cn/content/1195049.shtml
- http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=8364944
- https://www.actioncontrelafaim.org/a-la-une/tout-savoir-sur-lacces-a-leau-dans-le-monde/
- http://bluetechblog.com/2010/06/02/it%e2%80%99s-time-for-the-smart-water-grid/
- https://www.ecologie.gouv.fr/gestion-leau-en-france#:~:text=La%20politique%20de%20l'eau%20en%20France%20est%20fond%C3%A9e%20sur,est%20d%C3%A9coup%C3%A9%20en%2012%20bassins.
- https://www.aquatechtrade.com/news/water-treatment/singapore-smart-water-meters/
- http://swamp-project.org/
- https://www.infrastructure.gov.au/cities/smart-cities/collaboration-platform/Smart-Water-Management-Project-Illawarra-Shoalhaven.aspx
- https://www.sonepar.com/fr/actualites/detail/news/kvc-completes-two-water-treatment-projects-using-smart-water-management-solutions0.html
- https://enterpriseiotinsights.com/20171009/smart-cities/how-seoul-improved-waste-collection-via-smart-waste-management-tool-tag23-tag99
- https://www.iotconnect.io/IoT-smart-healthcare-solutions.html
- https://dataanalyticspost.com/securite-publique-que-dire-de-la-police-predictive/https://www.briefcam.com/
- https://tvilight.com/fr/
- http://www.rfidjournal.com/articles/view?4986
- http://senseable.mit.edu/trashtrack/
- https://www.lesechos.fr/idees-debats/cercle/opinion-google-city-de-toronto-les-raisons-dun-echec-1203831
- https://www.institutmontaigne.org/ressources/pdfs/publications/e-sante-augmentons-la-dose-rapport.pdf
- https://metropole.nantes.fr/charte-donnee
- https://en.wikipedia.org/wiki/Enterprise_service_bus
- https://www.sourcesecurity.com/insights/disruptive-innovation-providing-opportunities-smart-cities-co-1151-ga-co-3978-ga-sb.1618205981.html
- https://www.enedis.fr/open-data
- https://www.enedis.fr/professionnel-confidentialite-des-donnees
- https://www.strategie.gouv.fr/debats/couts-dinvestissements-financement-de-smart-city

- https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation
- https://www.ssi.gouv.fr/guide/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation/
- https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
- https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772?r=jM2u9JXwPZ
- https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/
- http://www.symantec.com/connect/blogs/dragonfly-western-energy-companies- under-sabotage-threat
- http://pjm.com/~/media/documents/reports/pjm-whitepaper-on-price-responsive-demand.ashx
- http://www.technologyreview.com/hack/414820/meters-for-the-smart-grid/.
- http://www.motherjones.com/politics/2013/08/chinese-hackers-attack-trend-micro-honeypots
- http://www.computerweekly.com/news/2240084537/Schoolboy-hacker-derails-Polands-tram- network
- http://www.ntsb.gov/doclib/reports/2010/RAR1002.pdf
- https://jhalderm.com/pub/papers/traffic-woot14.pdf
- http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html
- www.peregene.comwww.peregene.com
- https://club-ebios.org/site/wp-content/uploads/presentations/ClubEBIOS-2015-09-08-PERTUS.pdf
- https://hubinstitute.com/2019/Smart-City/transformation/decryptage-cybersecurit%C3%A9-smartcity
- https://www.datackathon.com/cybersecurite-villes-smart-city/
- https://www.labecedaire.fr/2019/04/23/smart-city-integrer-la-cybersecurite-des-la-conception/
- https://www.smartbuildingsalliance.org/cybersecurite-dans-batiment-et-ville-table-ronde-sba
- https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/smart-infrastructure
- https://www.ncsc.gov.uk/news/cyber-experts-set-out-blueprint-to-secure-smart-cities-of-the-future

- https://technative.io/how-smart-is-smart-city-cybersecurity/
- https://www.axis.com/blog/secure-insights/smart-city-cybersecurity/
- https://safesmart.city/en/cyber-attacks-smart-cities/
- https://www.smartcitiesdive.com/news/the-smart-city-tech-most-at-risk-for-cyberattacks-report/597365/
- https://ccdcoe.org/uploads/2020/12/6-Smart-Cities-Cyber-Warfare-and-Social-Disorder_ebook.pdf
- https://www.verdict.co.uk/smart-cities-cyberattacks-cybersecurity/
- https://www.analyticsinsight.net/futuristic-smart-cities-are-they-guarded-against-cybersecurity-threats/
- https://enterprise.verizon.com/resources/articles/s/securing-the-smart-city-of-the-future/
- https://www.rambus.com/iot/smart-cities/
- https://www.ishir.com/blog/9307/the-growth-of-smart-cities-and-why-cybersecurity-is-an-issue.htm
- https://www.ukauthority.com/articles/ncsc-publishes-principles-for-smart-city-security/
- https://us-cert.cisa.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf
- https://smartcity.press/iot-cybersecurity-threats-and-solutions/
- https://os.kaspersky.com/markets/smart-city/
- https://meetingoftheminds.org/cybersecurity-should-be-a-top-priority-for-smart-city-leaders-31241
- https://www.numerique.gouv.fr/espace-presse/le-gouvernement-annonce-sa-strategie-nationale-pour-le-cloud/

TABLEAU DES FIGURES