Club EBIOS

Les « *Smart Cities* » sous l'angle du risque cyber

Perspectives et challenges de demain

Thierry PERTUS

Septembre 2015

CONIX

AGENDA

- Contexte et modélisation du concept
- Perspectives de risques cyber
- Challenges de la cybersécurité

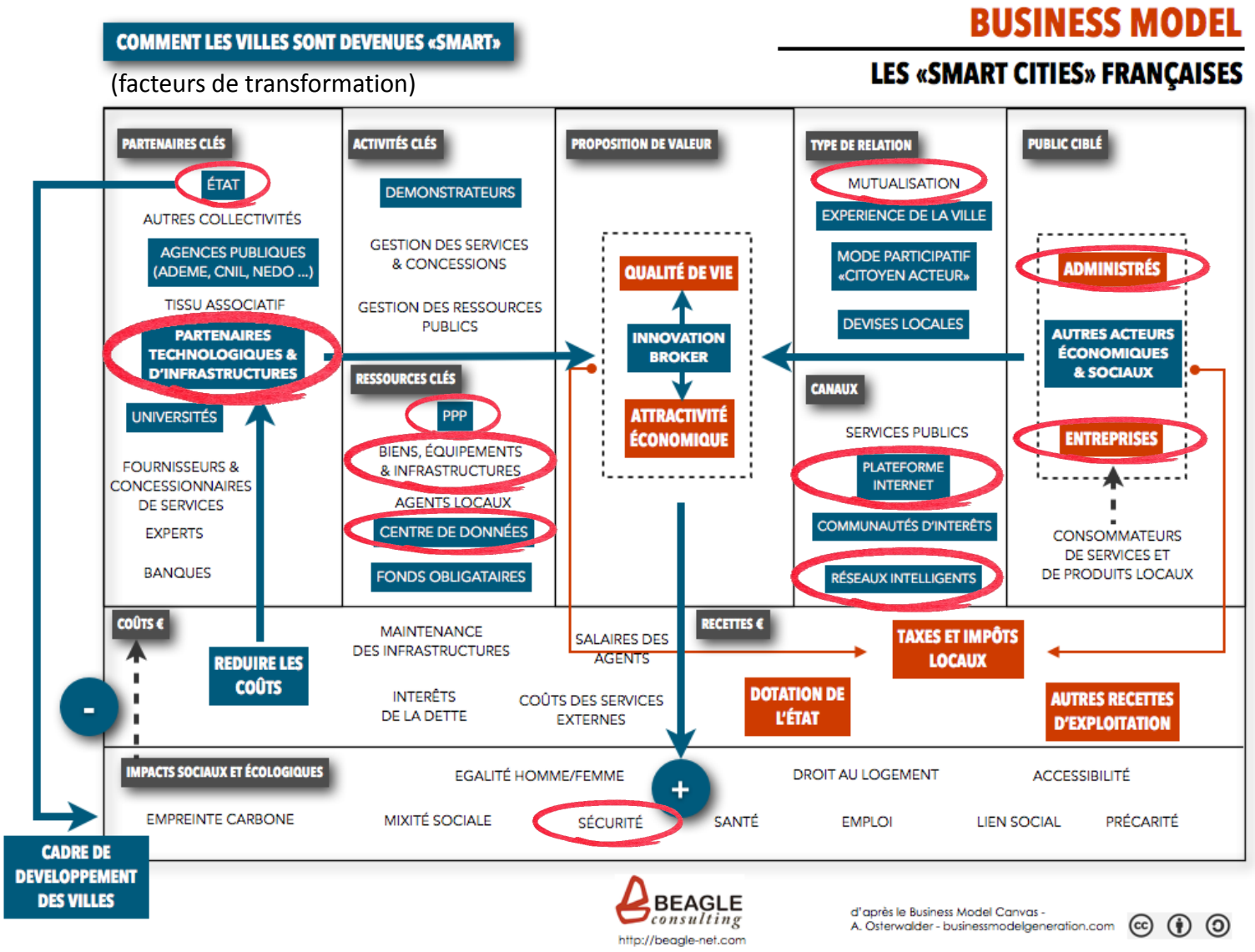
Contexte et modélisation du concept

Présentation des enjeux liés aux smart cities et des concepts sous-jacents

► Qu'entend-on par « *smart city* » ?

- ✓ Autres appellations : « **ville intelligente** », « **ville numérique durable** », « **ville interactive** », « **ville 2.0** »
- ✓ Concept introduit en 2005 par Bill Clinton à l'occasion d'un défi lancé par sa fondation à la firme Cisco Systems dans le but de concevoir des villes dites « durables » (source : Challenges)
- ✓ Désigne un **modèle systémique de développement urbain** apte à répondre, en s'appuyant sur les technologies de l'information et de la communication (TIC / ICT), à l'évolution ou l'émergence des besoins des institutions, des entreprises et des citoyens, tant sur le plan **économique**, **social**, qu'**environnemental** (source : Wikipedia)
- ✓ **Concept émergent** qui n'est pas encore clairement fixé, et dont le **caractère mouvant et ouvert**, rend complexe le passage à l'opérationnalité. (source : INTA)
- ✓ Deux conceptions s'affrontent néanmoins : « **technoville** » (modèle fonctionnel) *vs* « **écoville** » (modèle idéaliste)
  « *La ville intelligente, ce n'est pas que la ville de capteurs, la Tech City d'IBM ou Veolia, c'est la ville qui met l'humain au cœur* » Pierre Montel, fondation Territoires de Demain (ONG)

► Business model des « *smart cities* » dans notre contexte national



▶ Des tendances fortes et durables

- ✓ **Concentration de la population** en métropoles, voire en mégapoles (exode rural, densification urbaine)
- ✓ **Besoin d'attractivité des villes et des territoires** (rayonnement culturel, *competitivness benchmarking*)
- ✓ **Besoin exponentiel en hyper-mobilité et connectivité** (flexibilité, agilité, *anywhere anytime*)
- ✓ **Besoin d'efficience énergétique** (augmentation du coût de l'énergie, raréfaction des sources d'énergie fossiles, limitation des émissions de GES)
- ✓ **Besoin de redynamiser l'économie** (crise économique et sociale durable avec un taux de chômage qui atteint des records)
- ✓ **Augmentation du nombre de catastrophes naturelles** et des **coûts d'assurance** (dérèglement climatique)
- ✓ **Rôle grandissant des collectivités territoriales dans le cadre de développement durable** relayé par l'État (1er Sommet de Rio, grenelles de l'environnement, COP, éducation des populations, mode participatif)
- ✓ **Transfert progressif de compétences de l'État aux collectivités territoriales** (décentralisation)
- ✓ **Aggravation de la congestion du trafic automobile urbain** et de la **pollution de l'air en centre-ville**
- ✓ Evolution vers de **nouveaux modes de financement** : généralisation des partenariats public-privé (**PPP**)
- ✓ **Vieillissement de la population** (papy boom, augmentation de l'espérance de vie)

…

►Caractéristiques générales d'une ville qualifiée de « *smart city* » (finalités)

Selon **Rudolf Giffinger**, expert en recherche analytique sur le développement urbain et régional à l'université technologique de Vienne, les smart cites peuvent être classées d'après **6 critères principaux (piliers)**

SMART MOBILITY (Transport and ICT)

- Local accessibility
- (Inter-)national accessibility
- Availability of ICT-infrastructure
- Sustainable, innovative and safe transport systems

SMART ECONOMY (Competitiveness)

- Innovative spirit
- Entrepreneurship
- Economic image & trademarks
- Productivity
- Flexibility of labour market
- International embeddedness
- *Ability to transform*

SMART GOVERNANCE (Participation)

- Participation in decision-making
- Public and social services
- Transparent governance
- *Political strategies & perspectives*

SMART ENVIRONMENT (Natural resources)

- Attractivity of natural conditions
- Pollution
- Environmental protection
- Sustainable resource management

SMART LIVING (Quality of life)

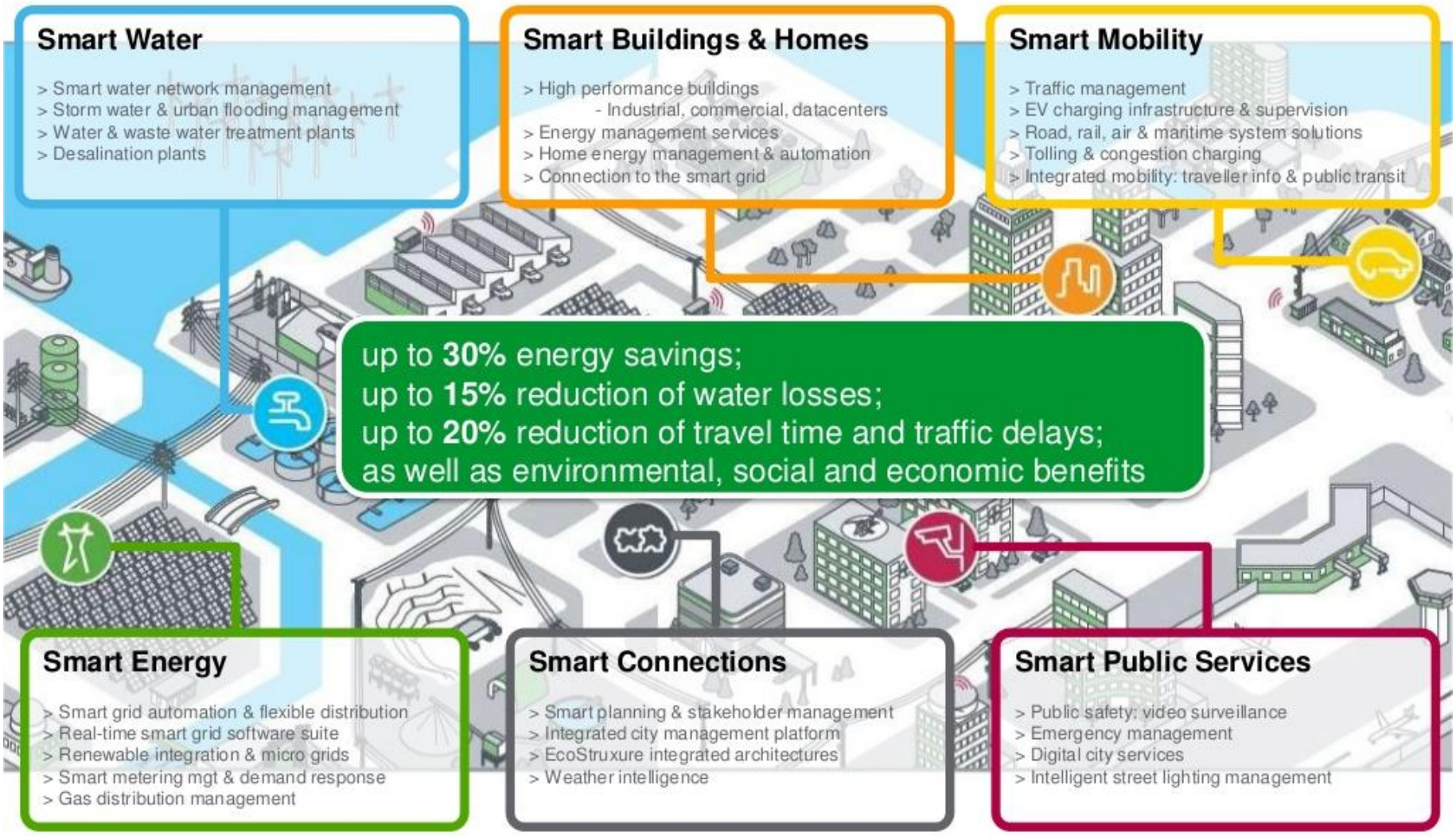
- Cultural facilities
- Health conditions
- Individual safety
- Housing quality
- Education facilities
- Touristic attractivity
- Social cohesion

SMART PEOPLE (Social and Human Capital)

- Level of qualification
- Affinity to life long learning
- Social and ethnic plurality
- Flexibility
- Creativity
- Cosmopolitanism/Open-mindedness
- Participation in public life

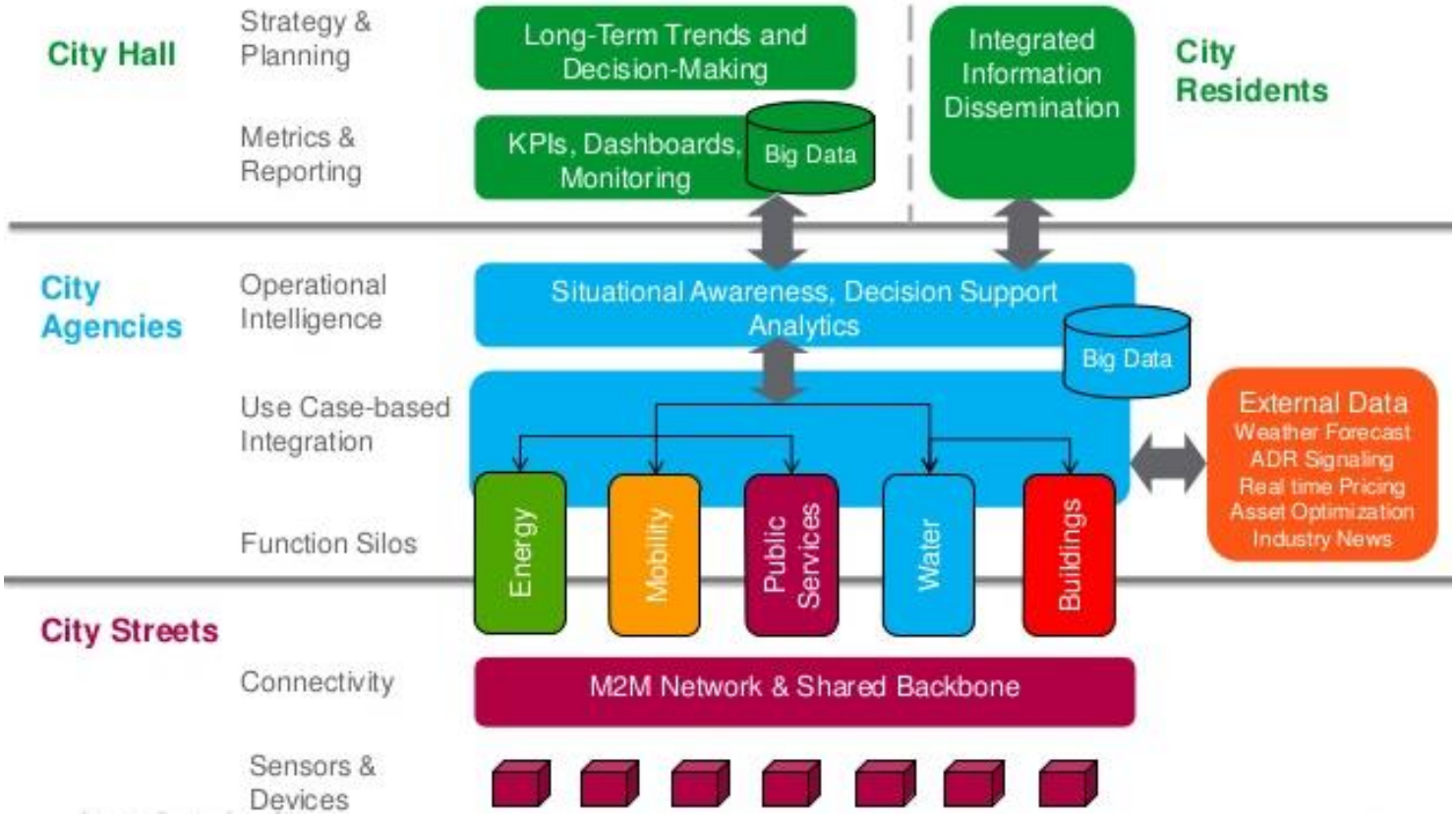
Source : European Smart Cities : the need for a place related Understanding - Rudolf Giffinger

► Building-blocks pour infrastructure efficiente (*smart infrastructure*)



Source : Seizing the Opportunity - Schneider Electric

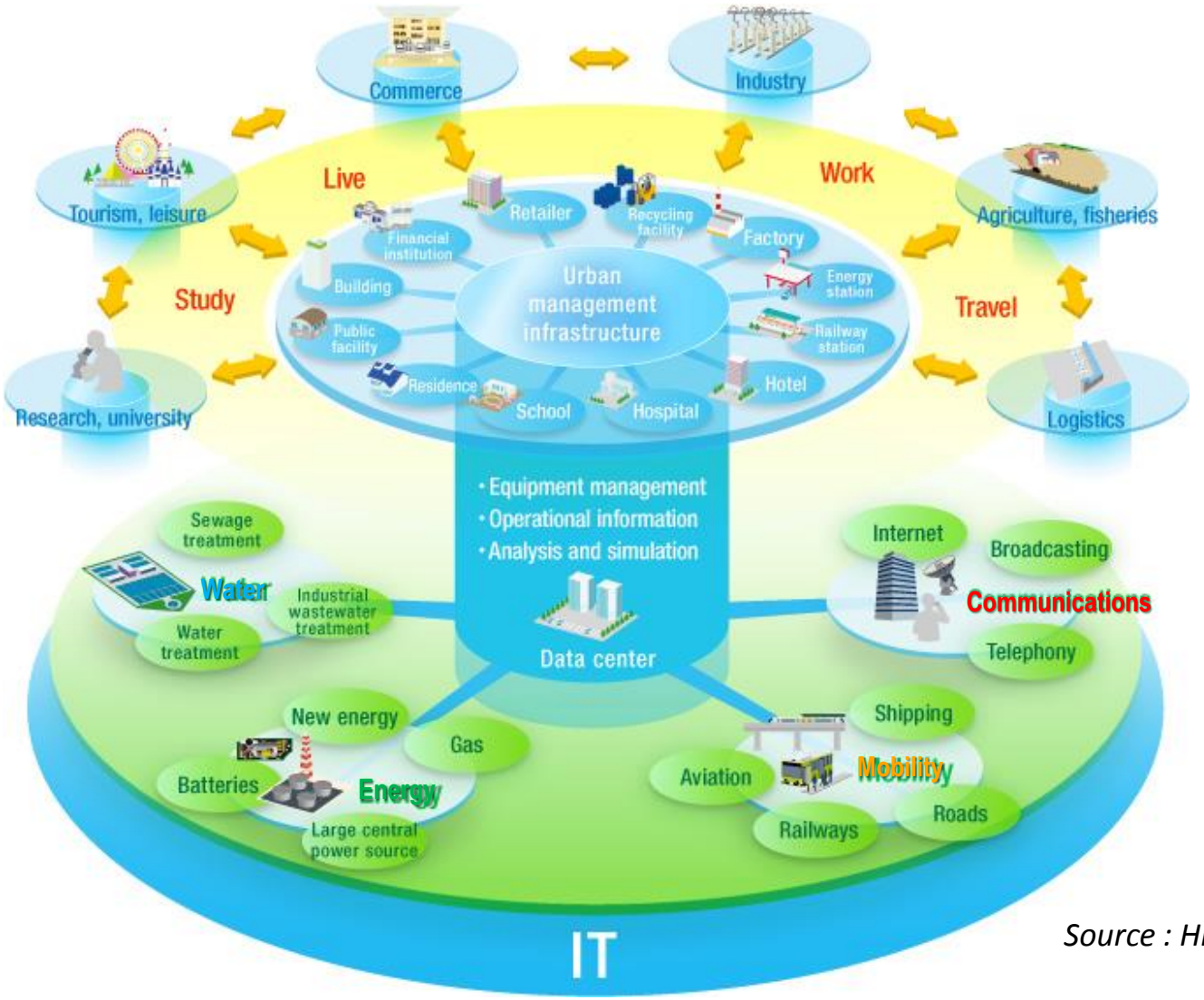
▶ Architecture fonctionnelle type d'une *smart city*



Source : Seizing the Opportunity - Schneider Electric

►Un framework ouvert

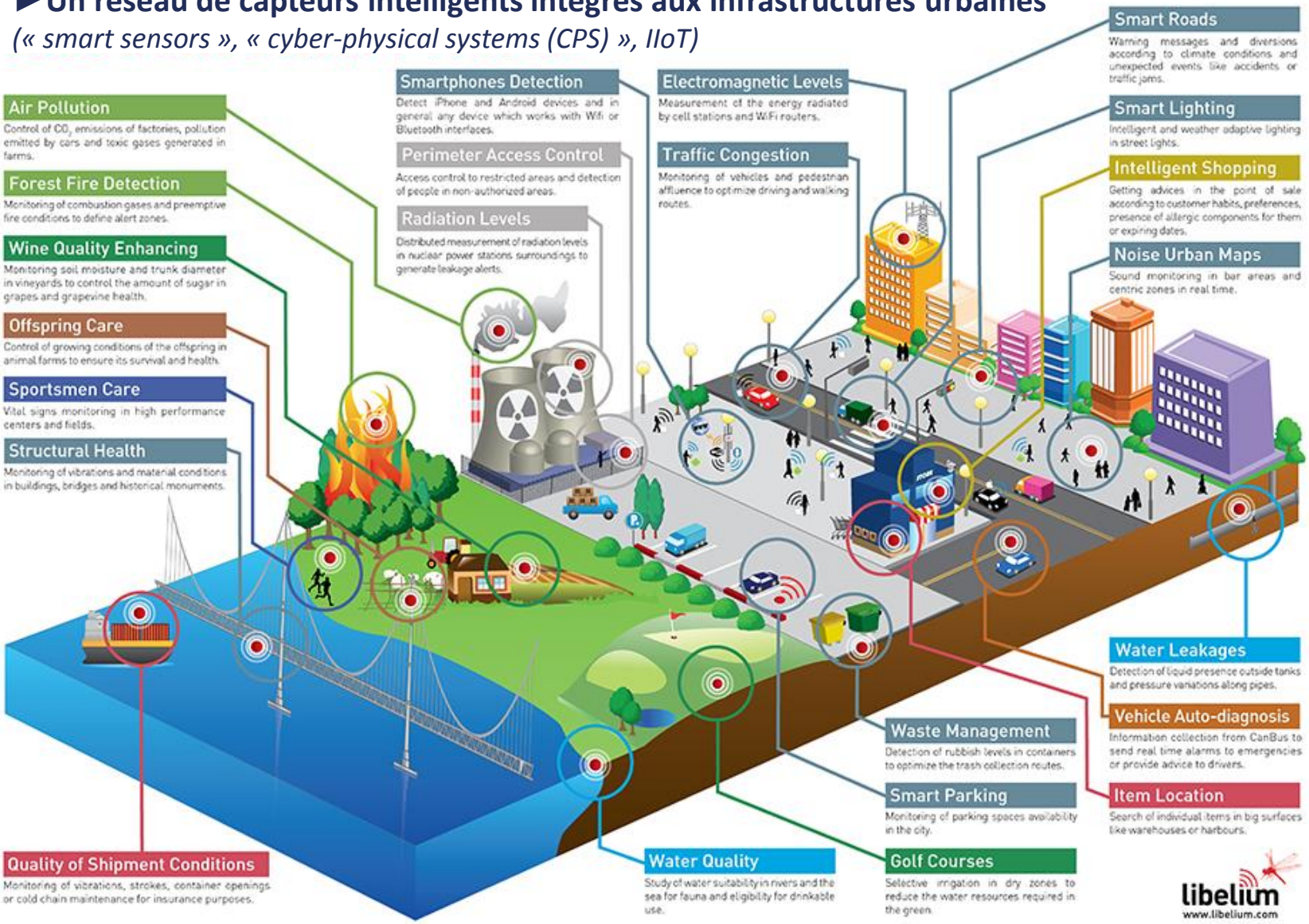
Une infrastructure numérique orientée services / fonctionnalités / géolocalisation



Source : Hitachi

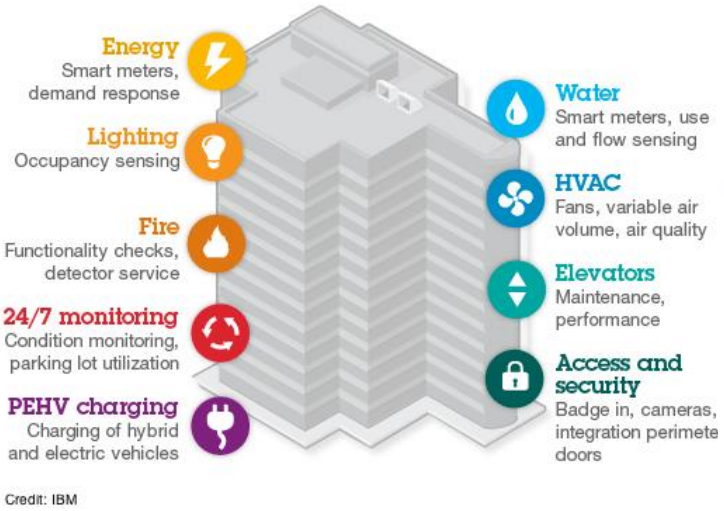
►Un réseau de capteurs intelligents intégrés aux infrastructures urbaines

(« smart sensors », « cyber-physical systems (CPS) », IIoT)



Source : Libelium : « Smart World » sensor applications

► Un modèle de *Smart building*



Source : reports.com

Source : nec.com

▶ Quelques *smart[er] cities* emblématiques dans le monde

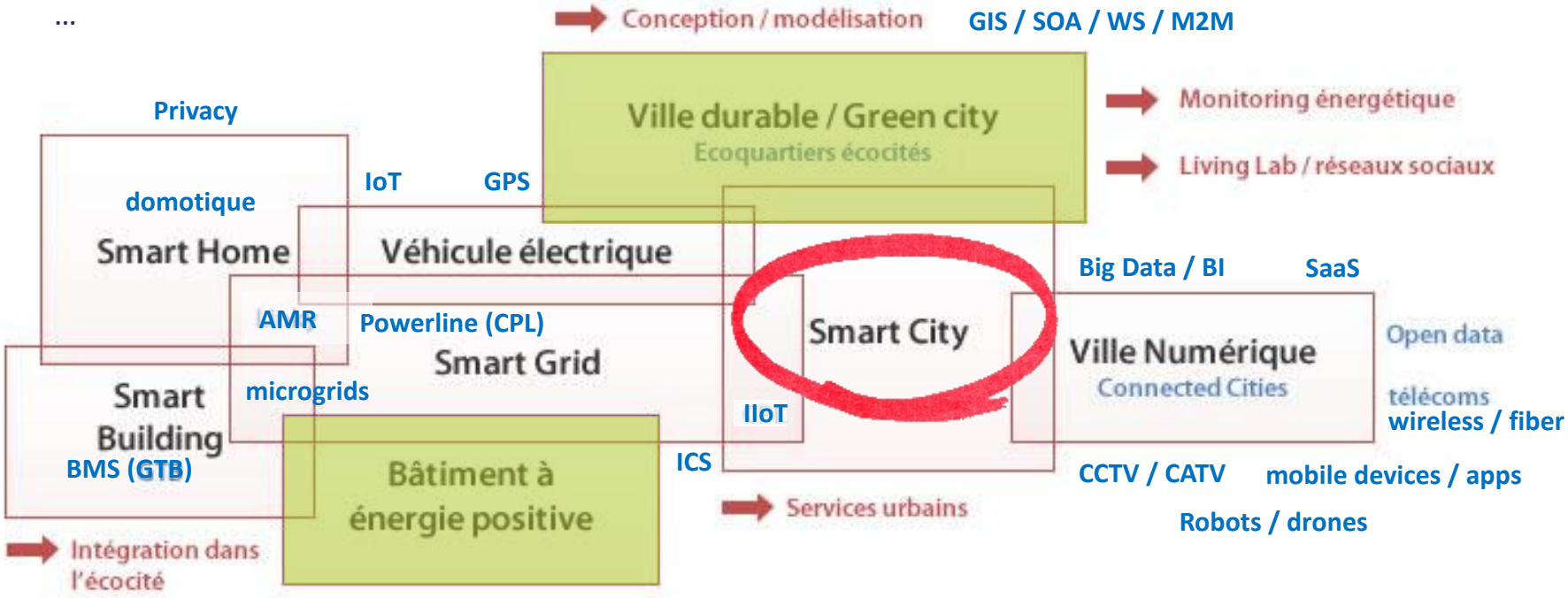
Perspectives de risques cyber

Prospective sur la base de scenarios de menaces potentiels

▶ Les technologies et les concepts connexes ou sous-jacents à la *smart city*

- ✓ **Banalisation du Cloud** (SaaS notamment) et systématisation de la dématérialisation des services
- ✓ **Banalisation des terminaux mobiles** (smartphones/tablettes)
- ✓ **Persistance de la connectivité sans fil** (4G, Wi-Fi, Bluetooth, RFID)
- ✓ **Emergence de l'Internet des objets** (IoT) avec les objets connectés, les drones, les échanges M2M
- ✓ **Accélération de la convergence IT / OT** (*Operational Technology*) > *Industrial Internet of Things* (IIoT)
- ✓ **Avènement du Big data**
- ✓ **Convergence** accrue entre **physique et virtuel** avec la **réalité augmentée** (smart glasses, smart textiles, …)

…



Source : inspiré de tecdev cité - ERDF

►Un cocktail explosif : le lourd héritage à porter par les *smart cities,* « à la croisée des chemins » en matière de vulnérabilités potentielles

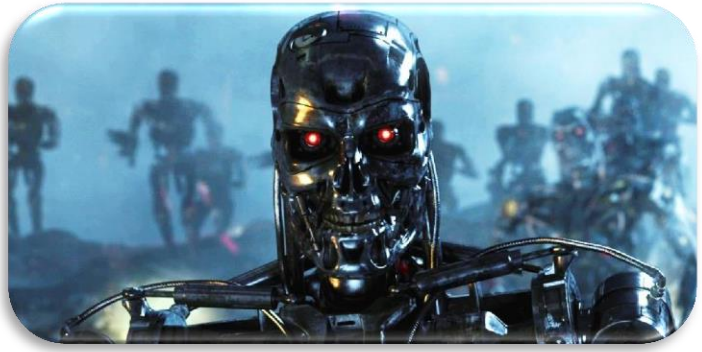
- **Surface d'attaque étendue et complexe** liée à l'hyper-connectivité (nombre de points d'accès et d'équipements communiquant, mobilité)
- **Maturité et capacité limitées** et des **systèmes industriels** (ICS) et des **capteurs intelligents** (IoT/IIoT) en matière de **cybersécurité** (ex : crypto)
- **Incertitude** quant à la **capacité de résilience et de réaction** de la part des infrastructures et des acteurs **en cas d'incident de sécurité sur les infrastructures critiques** (domaine de responsabilité, coopération pour les investigations et le retour en mode nominal)
- **Difficultés** en termes de **maintien en condition de sécurité** (**release and patch management**) d'un **parc hétérogène** ou **non évolutifs** (ICS) en matière de technologies déployées
- **Difficultés** pour imposer un **cadre de gouvernance privilégiant la cybersécurité** à l'innovation exacerbée
- **Confidentialité incertaine des données** lors de leur collecte / stockage / traitement centralisé (**Big data**, **IoT/IIoT**)
- **Attractivité accrue** liée aux **gains potentiels à l'échelle métropolitaine pour les cybercriminels** en puissance
- **Sécurité incertaine des applications en Cloud** ou **pour mobile**
- **Fiabilité incertaine** des divers types de **connectivité sans fil** (authentification mutuelle, chiffrement, persistance)
- **Volatilité des terminaux mobiles** jouant un **rôle pivot** pour l'usager (sujet à la perte et au vol par nature)
- …

Source : http://www.hldataprotection.com - NIST / Cyber Security Research Alliance (CSRA)

► Evènements « à redouter » avec à la clé des impacts aussi multiples que majeurs

« Massive Blackout »

« Big brother »



Syndrome « Skynet »

► Evènements « à redouter » avec à la clé des impacts aussi multiples que majeurs

- ***Blackout* énergétique** et/ou **télécom** suite à un **dysfonctionnement logiciel,** une **manipulation inappropriée,** une **opération de maintenance**, une **infection virale informatique** ou une **cyber-attaque**
- **Déviances** dans le cadre de la **collecte**, l'**exploitation** ou le **croisement de données à caractère personnel**
- **Perte de contrôle humain** préempté par les communications M2M ou lié à l'**extrême complexité** du **macro-système** à opérer et maintenir
- **Cyber-attaque** par **déni de service distribué** ciblant des **systèmes ou services urbains critiques**
- **Cyber-attaque intrusive** d'un **système de pilotage opérationnel** de **systèmes ou services urbains critiques**
- **Perturbation du trafic automobile** ou de **transport public** urbain
- **Manipulation illicite du paramétrage de capteurs ou d'actionneurs** de l'infrastructure urbaine
- **Propagation d'un logiciel malveillant** au sein ou au travers de l'infrastructure urbaine
- **Fuite ou exfiltration massive de données à caractères personnel** ou **de données sensibles** relative à l'**infrastructure ou aux services urbains**
- **Fraude informatique** par falsification de données de collecte
- **Usurpation d'identité numérique** d'un individu ou d'un objet connecté
- **Violation des obligations légales** ou **réglementaires**
- **Usage illicite ou inapproprié** de systèmes ou services urbains
- **Ecoute ou altération de communications** par **interception de transmission**
- **Récupération de données ou d'accès** suite à **perte ou vol de terminal mobile**
- **Emission** d'**informations erronées** auprès des **équipes de terrain** induisant des **interventions inappropriées à la situation**
- **Diffusion de fausses alertes** ou d'**informations erronées** aux **usagers de services urbains** induisant des **effets de panique**
- …

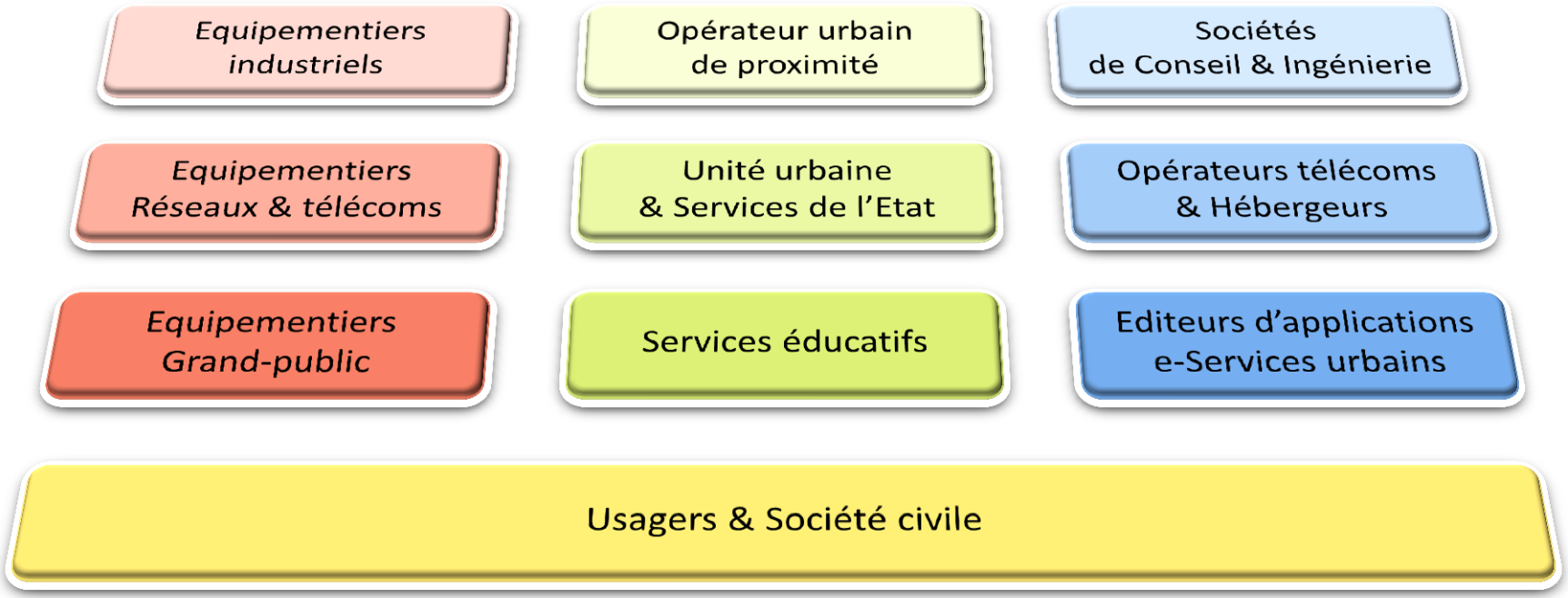
Source : Watch Dogs – gameplay 2014 (Ubisoft)

Challenges de la cybersécurité

Lignes directrices pour une cyber-résistance/résilience globale et efficiente

▶ Une multiplicité d'acteurs autour de la smart city

Chacun ayant un rôle à jouer à leur son respectif en tant que **partie prenante de la cybersécurité**

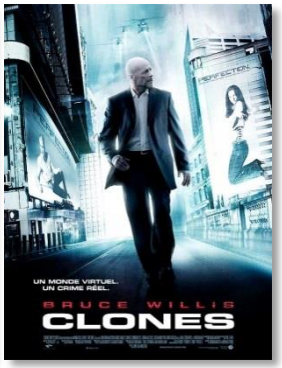


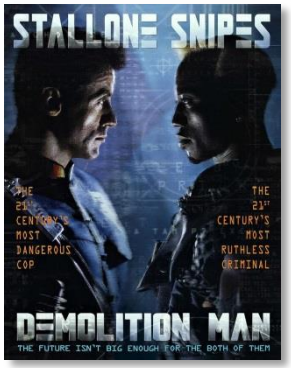
Source : inspiré de tecdev cité - ERDF

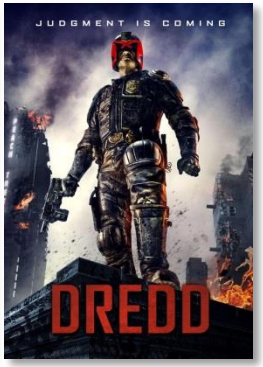
▶ Axes directeurs pour assurer la cybersécurité des smart cities

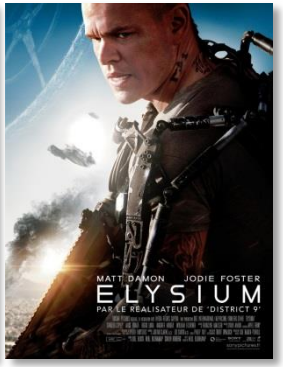
- ✓ Etablir un **cadre de gouvernance sous l'égide de l'Etat,** prenant en compte le **risque cyber**, assorti notamment d'une clarification des **rôles et responsabilités**, d'un **plan de gestion de crise** et de **revues de sécurité périodiques**
- ✓ Concevoir le **socle technique d'infrastructure urbaine** selon une **approche holistique** et **nativement sécurisé**, formaliser les **standards de sécurisation** en **fonction des technologies** et de leur **niveau de sensibilité**
- ✓ **Piloter les différents chantiers en intégrant la cybersécurité** sur l'ensemble du cycle projet
  1. Réaliser une analyse de risques en identifiant prioritairement les actifs sensibles
  2. Formuler les exigences fonctionnelles et veiller à leur déclinaison technique dans le respect des standards en vigueur
  3. Recetter la cybersécurité à la livraison des services et infrastructures, conditionnant la mise en production
  4. Contractualiser les engagements des fournisseurs et prestataires en matière de cybersécurité
- ✓ Assurer une **veille continue** sur les **vulnérabilités techniques** applicables et les **menaces émergentes**, **maintenir en condition de sécurité** les services et infrastructures critiques et de télémaintenance
- ✓ Assurer une **surveillance permanente**, **optimale** et **tracée** de toute activité suspecte et autres signaux faibles **dans le respect de la législation** en vigueur et **de façon déontologique**
- ✓ Etablir un **plan de continuité** en adhérence avec le plan de gestion de crise pour chacun des services et infrastructures critiques, planifier des **tests de résilience réguliers** pour en vérifier l'efficience
- ✓ Etablir un **plan de réponse à incident majeur** en adhérence avec le plan de gestion de crise, planifier des **exercices de simulation réguliers** à partir de scénarios préétablis pour en vérifier l'efficience
- ✓ **Sensibiliser régulièrement les intervenants et les usagers** sur les règles élémentaires et les bonnes pratiques en matière de cybersécurité en s'appuyant sur un **réseau de correspondants privilégiés**, instaurer une **culture de la sécurité** au travers des **cursus scolaires**
- ✓ Réaliser des **audits de sécurité réguliers** avec **tests d'intrusion** et **tests de charge** sur les services et infrastructures critiques et de télémaintenance par le biais de **plateformes de tests** ou autres **simulateurs hors production**, **piloter la mise en conformité** des écarts identifiés en priorisant par criticité

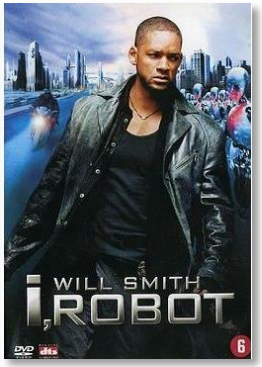
► **Filmographie** pour faire réfléchir sur les **modèles de** « **cités du futur** » imaginés par la fiction …

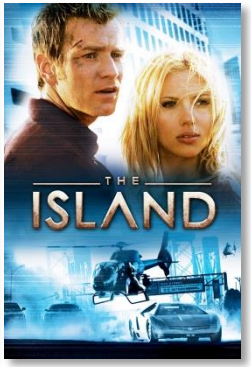


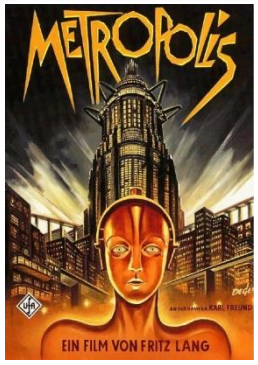


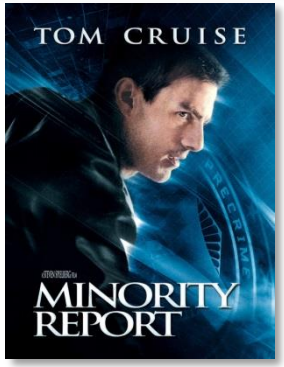












►Acronymes

CPL	Courant Porteur en Ligne
GTP	Gestion Technique du Bâtiment
PPP	Partenariat Public-Privé
SIG	Système d'Information Géospacial
TIC	Technologie de l'Information et de la communication

►Acronyms

AMR	Automated Meter Reading
BI	Business Intelligence
BMS	Building Management System
CPS	Cyber-Physical System
CATV	Community Access Television
CCTV	Closed Circuit Television System
GIS	Geospatial Information System
GPS	Global Positioning System
HVAC	Heating, Ventilation and Air-Conditioning
ICS	Industrial Control system
ICT	Information & Communication Technology
IIoT	Industrial IoT
IoT	Internet of Things
IT	Information Technology
M2M	Machine-to-Machine
OT	Operational Technology
PEHV	Plug-in Hybrid Electric Vehicle
PPP	Public-Private Partnership
RFID	Radio Frequency IDentification
SaaS	Software as a Service
SOA	Service-oriented Architecture
WS	Web Services

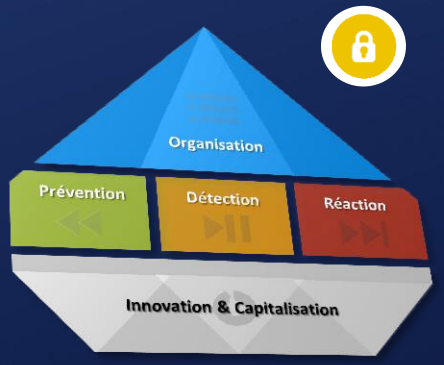
CONIX

Cybersécurité

securite@conix.fr

www.conix.fr

Merci de votre attention



Powered by CONIX