digital security | econocom

4.0 INDUSTRIES DU FUTUR
Mulhouse • 14 et 15 juin 2017

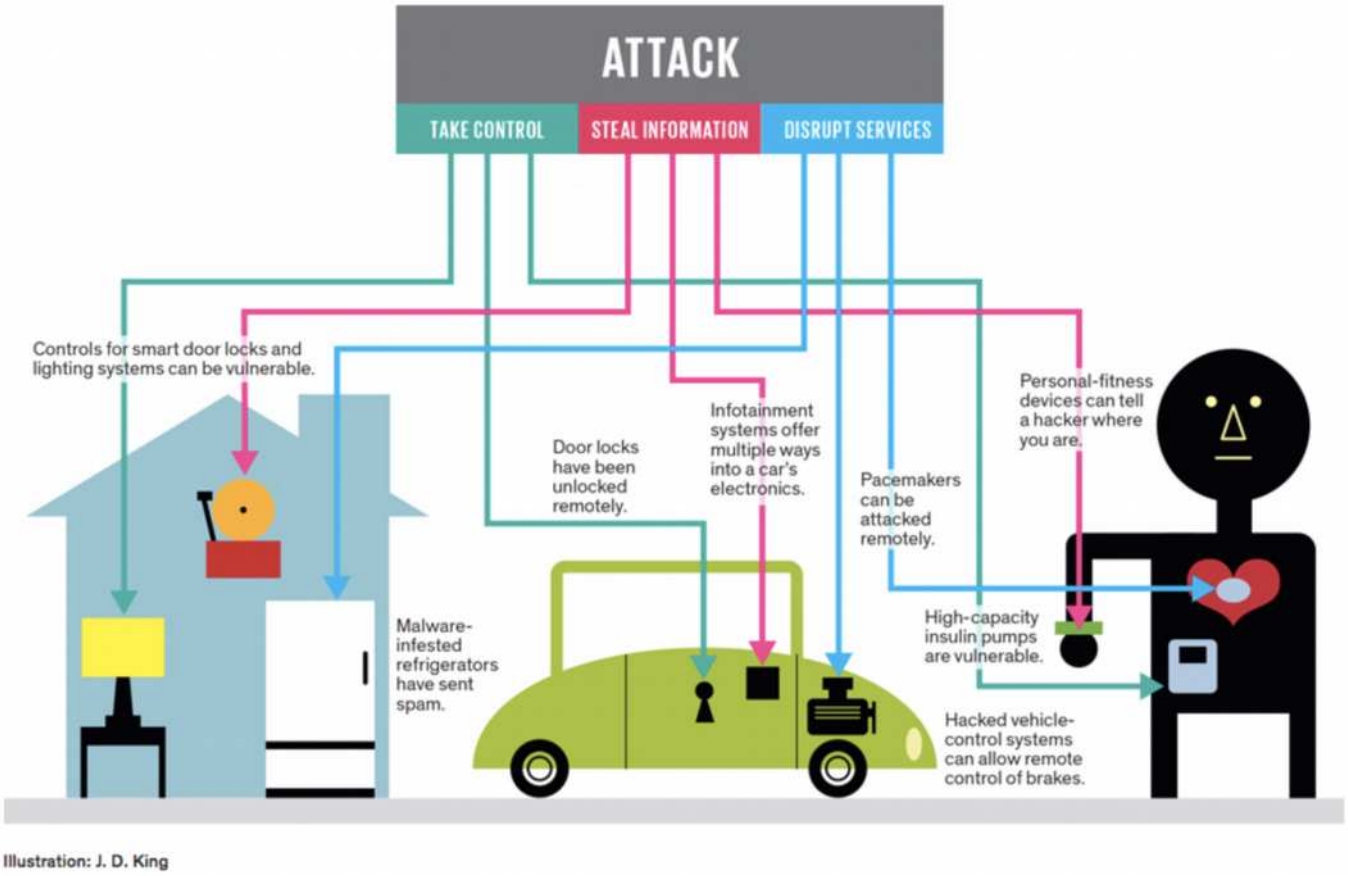
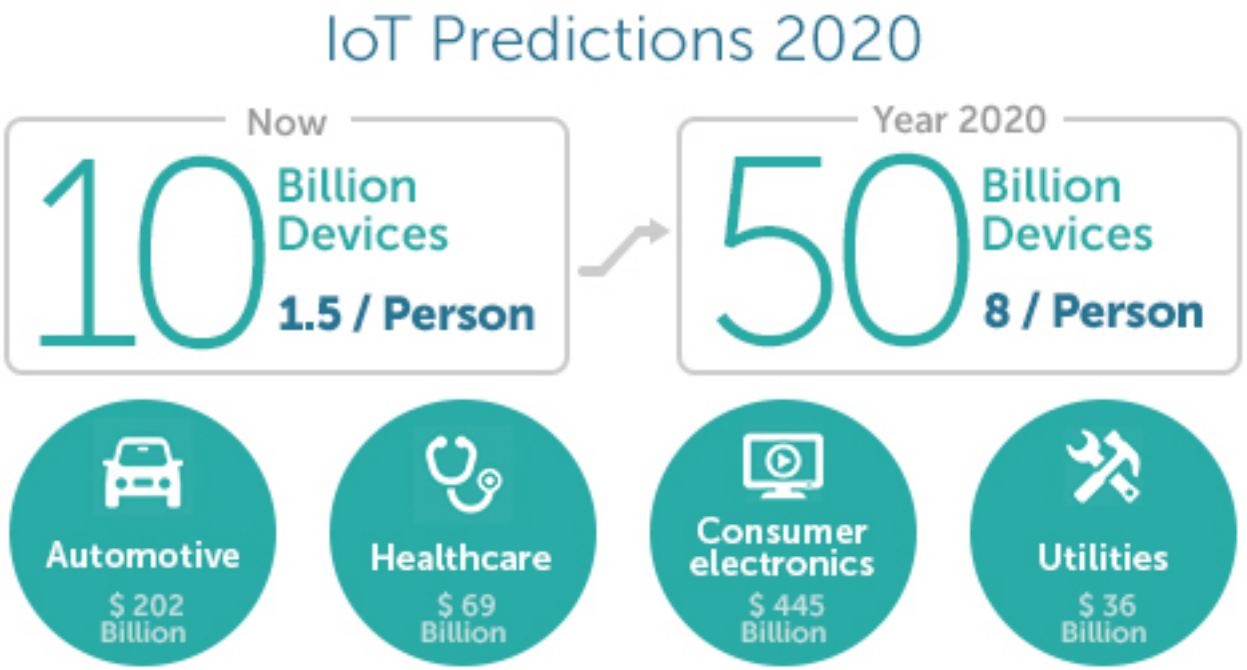


Illustration: J. D. King

Sécurité dans l'Internet des objets

Salon Industries du Futur 2017 – Mulhouse – 14 & 15 juin 2017

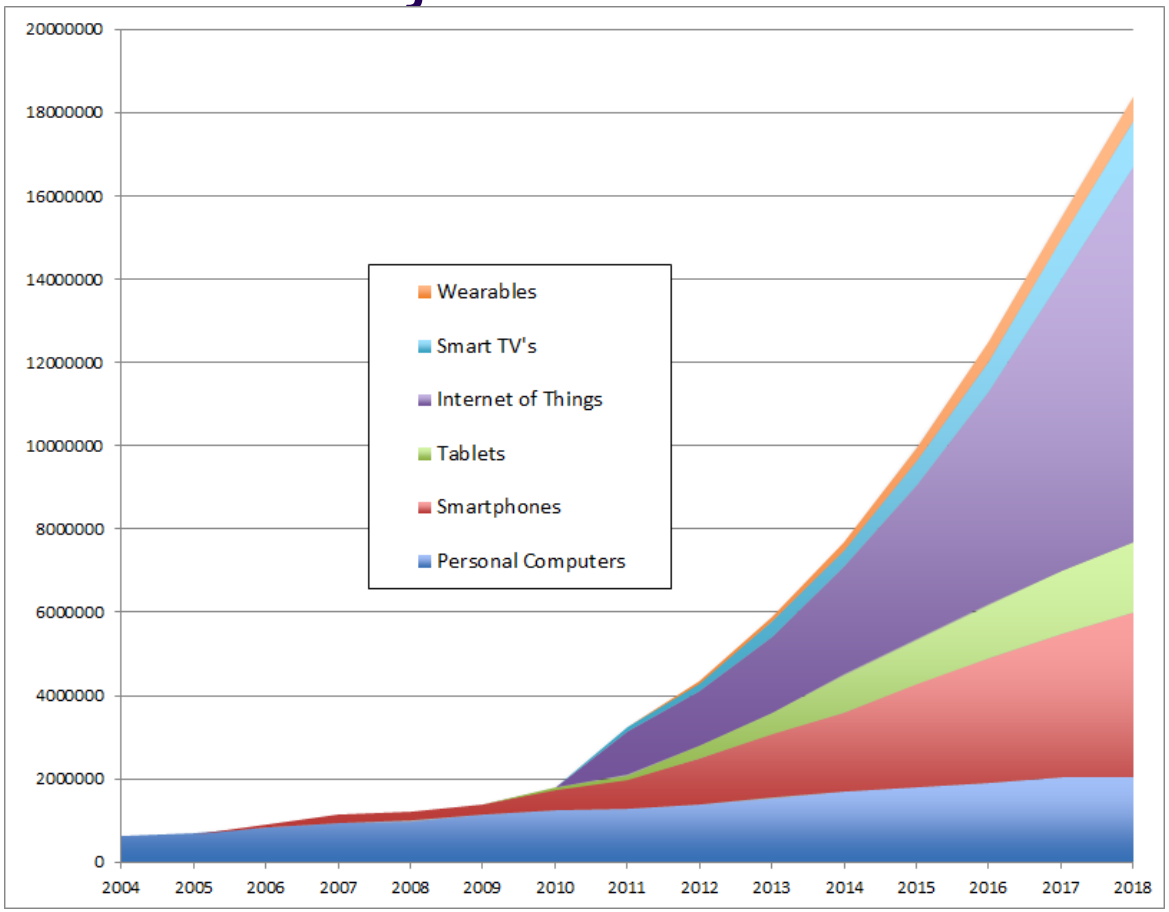
Adoption des objets connectés



Source : iot-analytics.com

- Gartner :
  - « **D'ici la fin de l'année 2017, 20% des entreprises auront des équipes de sécurité dédiées** à la protection de leurs activités utilisant les services et équipements IoT »

Adoption des objets connectés



Source : kaizen-factory.com

Les nouveaux objets connectés représenteront dans 2 ans la moitié des équipements connectés à Internet

Définition

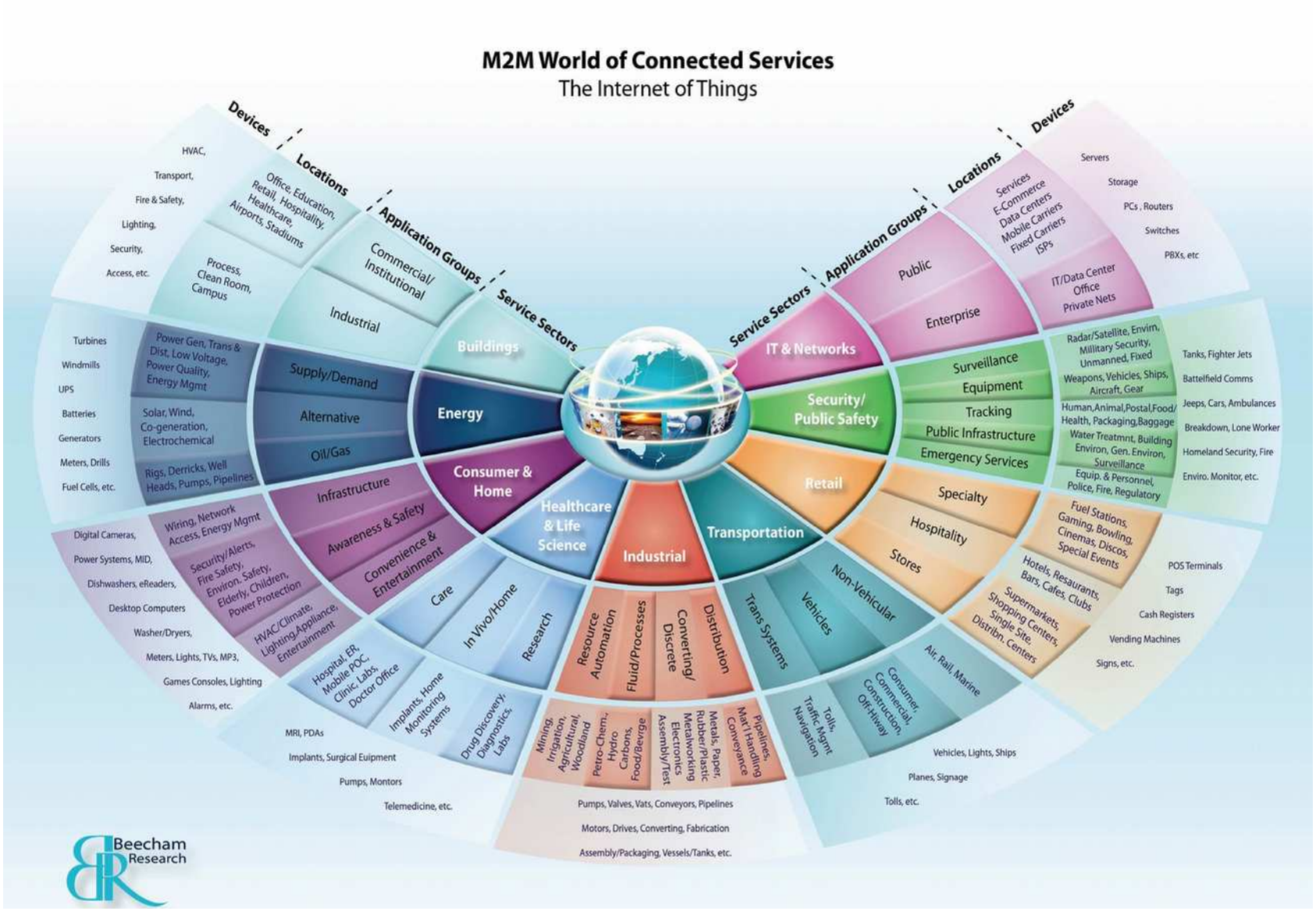
- L'IoT-GSI définit l'Internet des objets :
  - *une infrastructure mondiale permettant d'offrir de services évolués en interconnectant des objets physiques ou virtuels grâce à l'interopérabilité des TIC.*

- L'IoT-GSI définit un objet connecté comme un équipement possédant les sept attributs suivants :
  - Capteur
  - Connectivité à Internet
  - Processeur
  - Efficacité énergétique
  - Cout optimisé
  - Fiabilité
  - Sécurité

Acteurs

- 3 acteurs principaux dans la mise en œuvre d'une solution connectée :
  - Les créateurs de solutions connectées
  - Les opérateurs de communications
  - Les opérateurs de service d'appui (stockage et traitement des données)

Tous les secteurs d'activité sont concernés

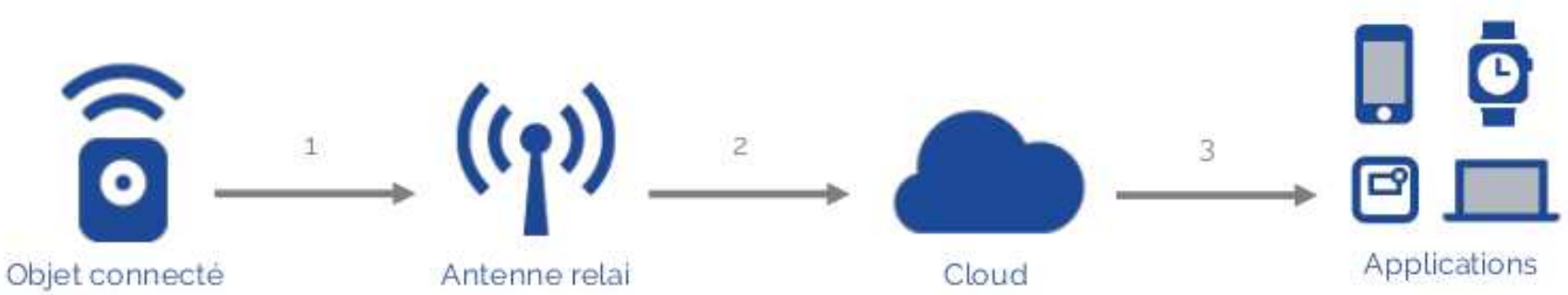


Anatomie d'un objet connecté

- Un élément physique
- Un ou plusieurs SoC (System-On-Chip)
  - Mémoire programmable, micro-processeurs, entrées/sorties
  - Bus de communication SPI, I2C, UART
- Micrologiciels et systèmes d'exploitations
  - Systèmes de fichiers, environnement multitâche

Infrastructure LPWAN

- Réseaux LPWAN (Low Power Wide Area Network)

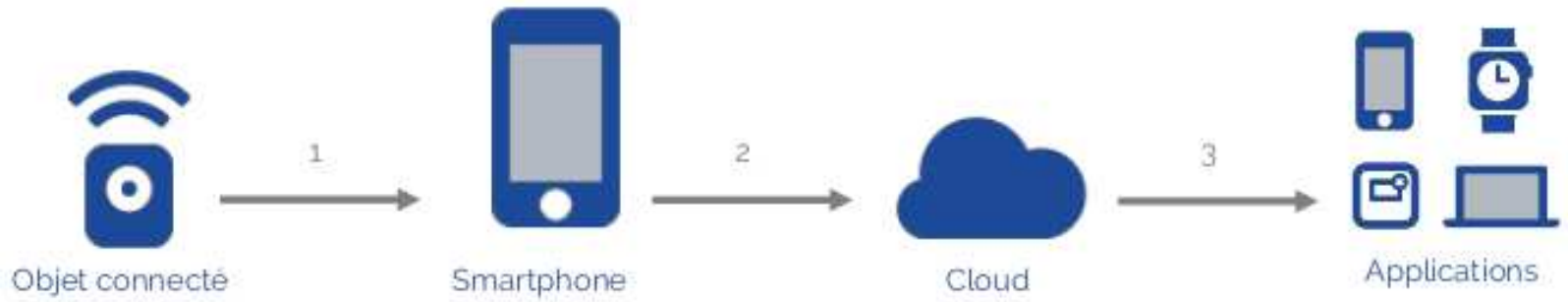


1 – Envoi des données recueillies de l'objet à une antenne relai (LoRa, Sigfox, GSM…)
2 – Relai des données de l'antenne vers le Cloud
3 – Retransmission des données vers les applications (mobile, gadget, web…)

LoRa®
SIGFOX One network A billion dreams
QOWISIO ULTRA NARROW BAND
Lte
5G

Infrastructure de courte portée

- Réseaux de courte portée compatibles smartphones



1 – Envoi des données recueillies de l'objet à une antenne relai (LoRa, Sigfox, GSM…)
2 – Relai des données du smartphone au serveur du constructeur (WiFi, GSM…)
3 – Retransmission des données vers les applications (mobile, gadget, web…)

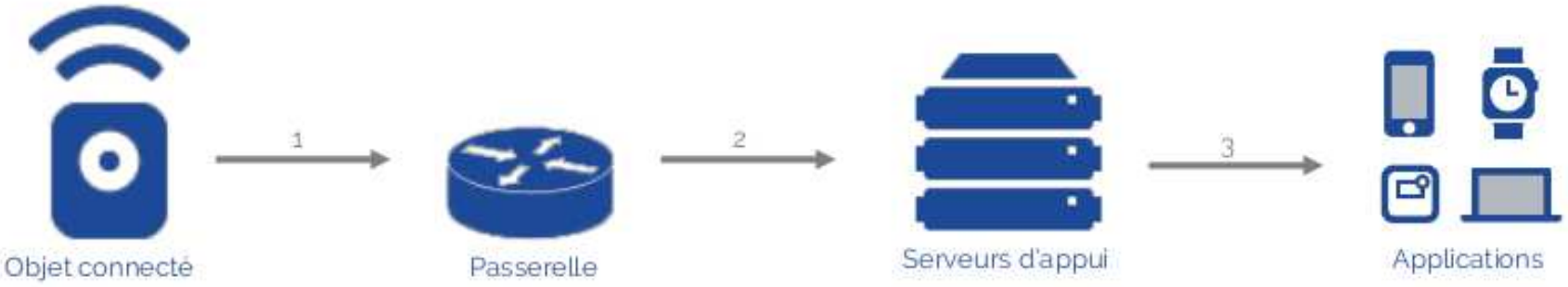
Bluetooth® SMART

RFID

Wi Fi

Infrastructure « relais »

- Réseaux de courte portée utilisant une passerelle locale



1 – Envoi des données recueillies de l'objet à la passerelle de l'utilisateur (ZigBee, Z-Wave, Wifi, etc...)
2 – Envoi des données de la passerelle aux serveurs d'appui (Box internet, GSM+, etc...)
3 – Retransmission des données vers les applications (mobile, gadget, web...)

ZigBee® LoWPAN IPv6-based Low-power Wireless Personal Area Networks Z-WAVE enocean®

Des solutions techniques très hétérogènes

- Systèmes d'exploitation peu ou pas connus
  - FreeRTOS, Lepton, REMS, RIOT, TinyOS, Contiki, eCos
  - Brillo (Google), LiteOS (Huawei), Windows 10 IoT Core (Microsoft), Mbed OS (ARM)

- Normes de radiofréquence
  - Wifi, Bluetooth LE, NFC, RFID
  - SigFox, LoRa, LoRaWAN, Qowisio, ZigBee, Z-Wave, 6IoWPAN, EnOcean, Normes propriétaires

Absence de référentiels de sécurité

La démocratisation de l'IoT, source de menaces pour les données personnelles

- Exploitation d'un volume gigantesque de données personnelles => Big Data
  - 44 milliards de gigaoctets de données en 2020 soit 10 fois plus qu'en 2013
  - 50 000 gigaoctets = volume de données créé par seconde en 2020 contre 100 gigaoctet en 1992

- Remise en question de la sécurité des données personnelles
  - Marché lucratif pour les criminels => revente de données sur le darknet
  - Compromission de données personnelles via les ransomwares
  - Espionnage abusif des entreprises

Scénarios redoutés … et réalisés

digital security

Cyberattaque sur les systèmes de contrôle d'accès

- Piratage des serrures connectées (domotique) par le biais de vulnérabilités de l'objet ou du cloud

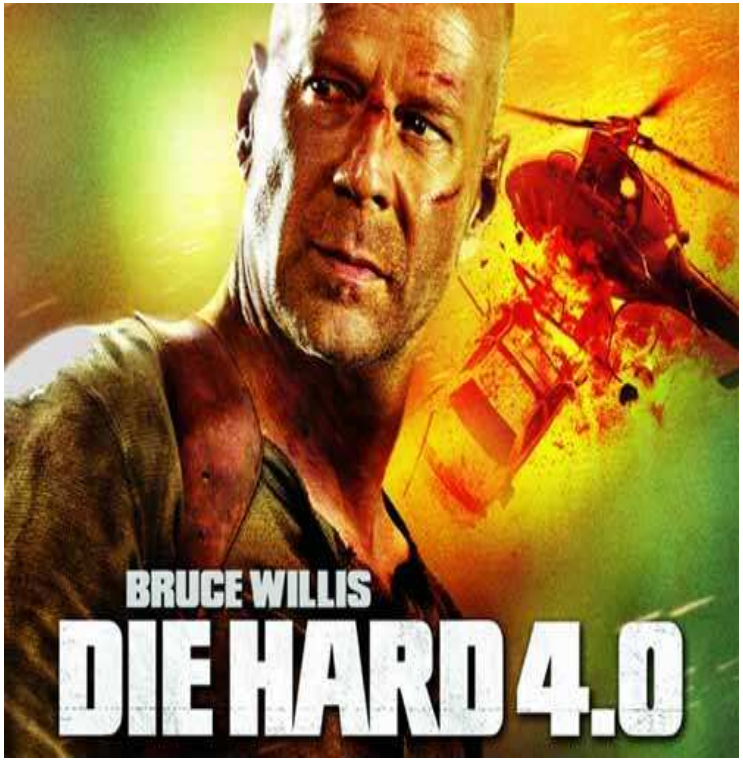
Compromission IoT médicaux

- Vol de données médicales dans un dossier patient (ransomwares)
- Compromission massive d'équipements médicaux connectés

Smart City : Déstabilisation d'une métropole (*Die Hard style*)

- Blackout d'une smart city : pannes, accidents de la circulation, pannes dans les hôpitaux

- Contamination de l'eau via une cyberattaque contre les usines de traitement de l'eau



Drones d'attaques

- Scénario n°4 – Préparation d'opérations terroristes à l'aide aux drones
  - Repérage d'infrastructures critiques par des drones
  - Transports de substances explosives

digital security | econocom