L'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information

Autorité nationale en matière de sécurité des systèmes d'information

2 sites à Paris

Hôtel National des Invalides

Quai de Grenelle

550 agents civils et militaires

Positionnement de l'ANSSI

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Services du Premier Ministre

SGDSN
Secrétariat Général de la Défense et de la Sécurité Nationale

Coordination interministérielle en matière de défense et de sécurité nationale

ANSSI
Agence Nationale de Sécurité des Systèmes d'Information

Autorité nationale en matière de sécurité et de défense des systèmes d'information

Créée le 7 juillet 2009 par le décret n°2009-934, l'ANSSI est un **service à compétence nationale.**

Le modèle français

-> Autorité de sécurité (prévention)

-> Autorité de défense (réaction)

-> Police
-> Actions judiciaires

-> Renseignement
-> Actions offensives

L'ANSSI porte aussi la voix de la France à l'étranger en matière de cybersécurité

Grandes missions

- **Réglementation**

- **Visas de sécurité**
  (*qualifications et certifications de produits et services*)

- **Conseils, sensibilisation et soutien**

- **Réseaux sécurisés gouvernementaux**

- **Supervision & Défense**

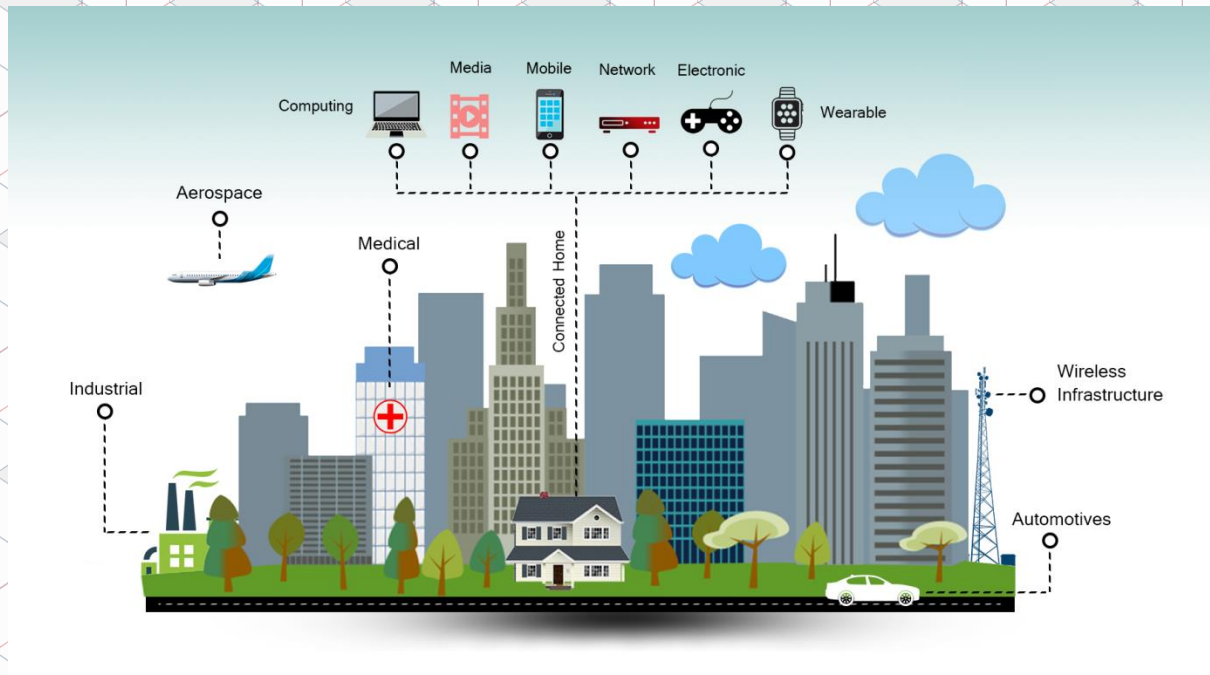
Principal périmètre d'intervention : institutions, ministères et OIV

ETAT DE LA MENACE CYBER

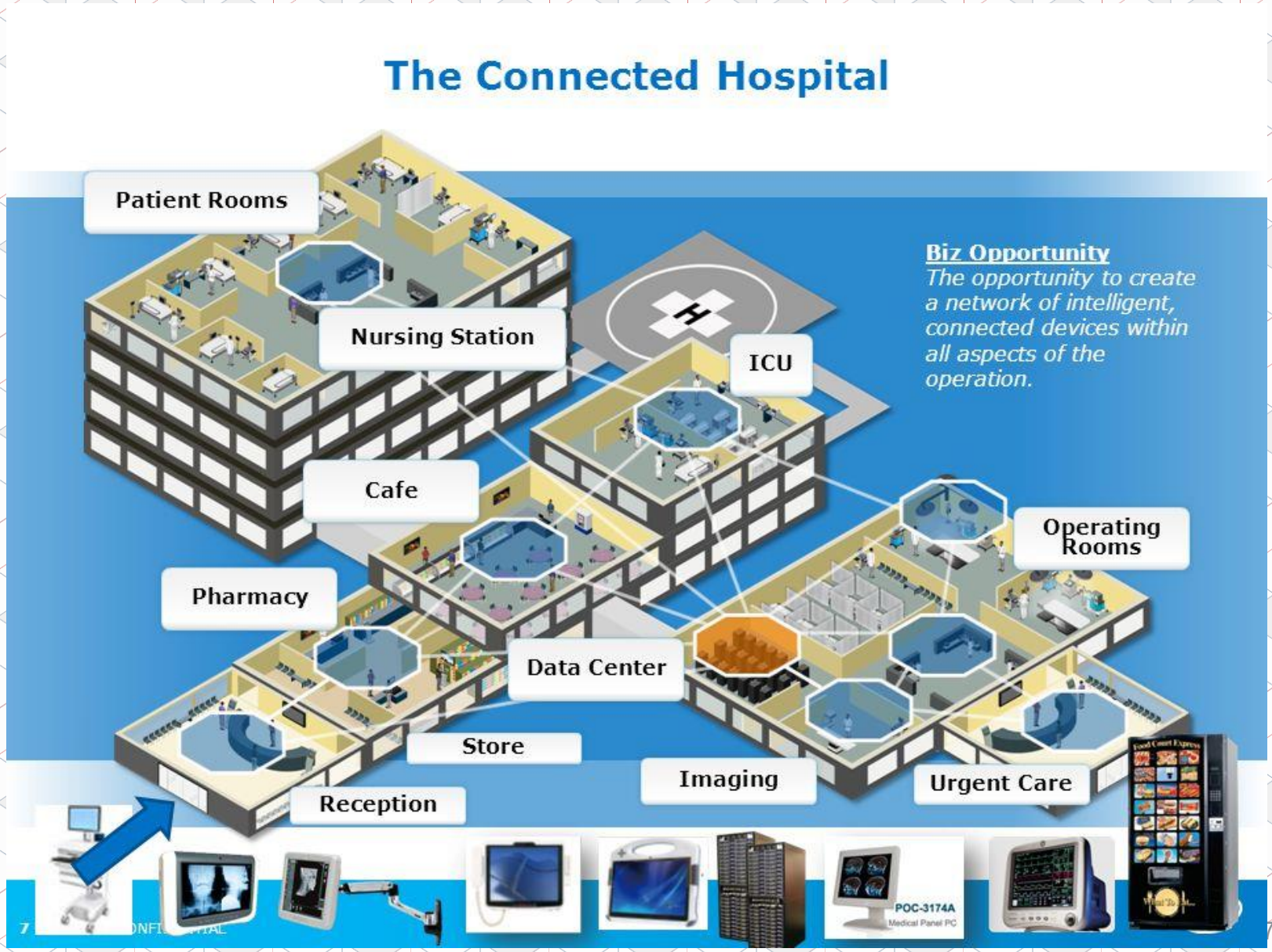
L'INTERNET DU FUTUR : LES OBJETS CONNECTÉS

En 2017, 27 milliards d'objets connectés

En 2030 , 125 Milliards



UN EXEMPLE : L'HOPITAL CONNECTÉ

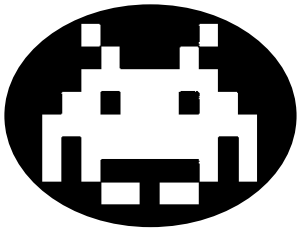


Consequences

- Les coûts économiques des cyber-attaques à grande échelle dépassent déjà les dégâts causés par les catastrophes naturelles.

Finalités poursuivies

ESPIONNAGE

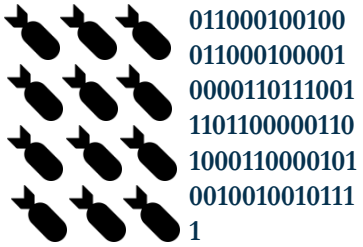


PRÉ-POSITIONNEMENT (INVASION)

AGITATION - PROPAGANDE

DESTRUCTION

FRAUDE



NEUTRALISATION

Grandes catégories d'attaque

➢ VOIE NUMERIQUE

- Ver, virus, cheval de Troie,
- *Keylogger*, porte dérobée,
- Usurpation de trames,
- Bombe logicielle,
- Saturation réseau,
- Neutralisation

➢ VOIE COGNITIVE

- Manipulation :
- à distance (ciblée ou de masse),
- au contact (interne)

➢ VOIE PHYSIQUE

- Effraction (salle serveur),
- Destruction (câbles),
- Piégeage (PABX, Ecran)

Pourquoi les attaques réussissent-elles trop souvent ?

1) Systèmes et applications pas à jour dont sites Web
2) Politique de gestion des mots de passe insuffisante
3) Pas de séparation des usages (utilisateur/administrateur) et des réseaux
4) Laxisme dans la gestion des droits d'accès
5) Absence de surveillance des SI
6) Pas d'anticipation des menaces souvent pour des raisons financières
7) Cloisonnement insuffisant des systèmes (propagation latérale)
8) Absence de restrictions (périphériques…)
9) Nomadisme / télétravail incontrôlés
10) **Sensibilisation et maturité insuffisantes des utilisateurs**

Pour conclure provisoirement…

80 %

Des attaques n'auraient pas abouti par :

- l'application de mesures simples de sécurité
- une sensibilisation des collaborateurs

On parlera d'hygiène informatique

ou d'*hygiène numérique*