LA SÉCURITÉ D'UN CAMPUS UNIVERSITAIRE

E.CASSETTE – RSSI LILLE1

SOYONS PRECIS
C'est à quel sujet ?

Sécurité d'un campus universitaire

Sécurité : des systèmes d'information

- **simple oubli ou lapsus inconscient ? : peut-on comparer le management de la sécurité d'un S.I. à celle de la sécurité physique ? (vous avez 4 heures)**

d'un campus universitaire : système hétérogène → indiquer les particularités par rapport aux autres environnements ESR (école, labo)

Remarques :

- **Vision subjective (celle du RSSI)**
- **Risque : embellir (syndrome du « c'est mieux chez les autres »)**

RAPPELS ?...
On ne parlera pas de

Audience = administrateurs de systèmes informatiques

➔ bien au courant des bonnes pratiques SSI

Donc, inutile de rappeler les bases de la SSI :

- **engagement de la direction à sécuriser son SI (« sponsoring »),**
- **définition du périmètre concerné,**
- **énoncé des objectifs de sécurité macroscopiques (Politique SSI),**
- **connaissance des éléments de son SI (cartographie),**
- **connaissance des vulnérabilités et des menaces (analyse de risques),**

…RAPPELS ?…
On ne parlera pas de

- définition des acteurs de la SSI et des circuits d'information (AQSSI, FSD, CIL, RSSI, Correspondants SSI, experts SSI, relations avec RENATER, Ministères, ANSSI, CNIL…),
- définition des « règles du jeu » pour les diverses catégories de personnels ou d'usagers (règlement d'usage du SI pour les utilisateurs, charte pour les administrateurs de systèmes informatiques, charte RENATER, …)
- mise en œuvre des mesures de sécurisation nécessaires et suffisantes par rapport au risque,
- contrôle à postériori,
- remise en question régulière (hop, un tour de roue),

...RAPPELS ?

On ne parlera pas de

Remarque : il faudrait entre 4 à 5 ETP pour réaliser tout ça (1 RSSI, 1 RSSI Suppléant, 1 ou 2 experts, 1 EBIOS-man / auditeur)

Et puis, c'est beaucoup plus facile à dire qu'à faire...

PARTICULARITÉS SSI CAMPUS…

On n’est pas normal ?

Déjà dans un environnement "normal", s'occuper de SSI n'est pas une sinécure. Alors, dans un campus universitaire…

Pourquoi ?

Avertissement : les propos qui vont suivre ne seront pas politiquement corrects

…PARTICULARITÉS SSI CAMPUS…
On n'est pas normal ?

1) Un campus universitaire est un milieu très hétérogène

- structures,
- personnes,
- motivations,
- tutelles,
- sensibilités et politiques SSI,
- hiérarchies,
- sources de financement et contraintes budgétaires,
- charges de travail, stress.

…PARTICULARITÉS SSI CAMPUS…
On n'est pas normal ?

2) Un campus universitaire a très peu de contraintes de rentabilité économique, et une forte tradition de « liberté académique », ce qui augmente le champ des réactions possibles

- **on peut dire « -faite ceci » ou « -ne faite pas cela », mais les probabilités que ça soit respecté sont assez faibles,**
- **les personnels sont allergiques aux règles qu'ils estiment non justifiées (qualifiées d'arbitraires), la confiance « à priori » n'est pas acquise,**
- **on ne peut pas (beaucoup) compter sur le pouvoir hiérarchique N/N+1, encore moins sur celui des RSSI (« -de quoi j'me mêle ?- ») ; utiliser ce pouvoir est considéré comme un aveu d'impuissance,**
- **les procédures de sanction sont rarement mises en œuvre.**

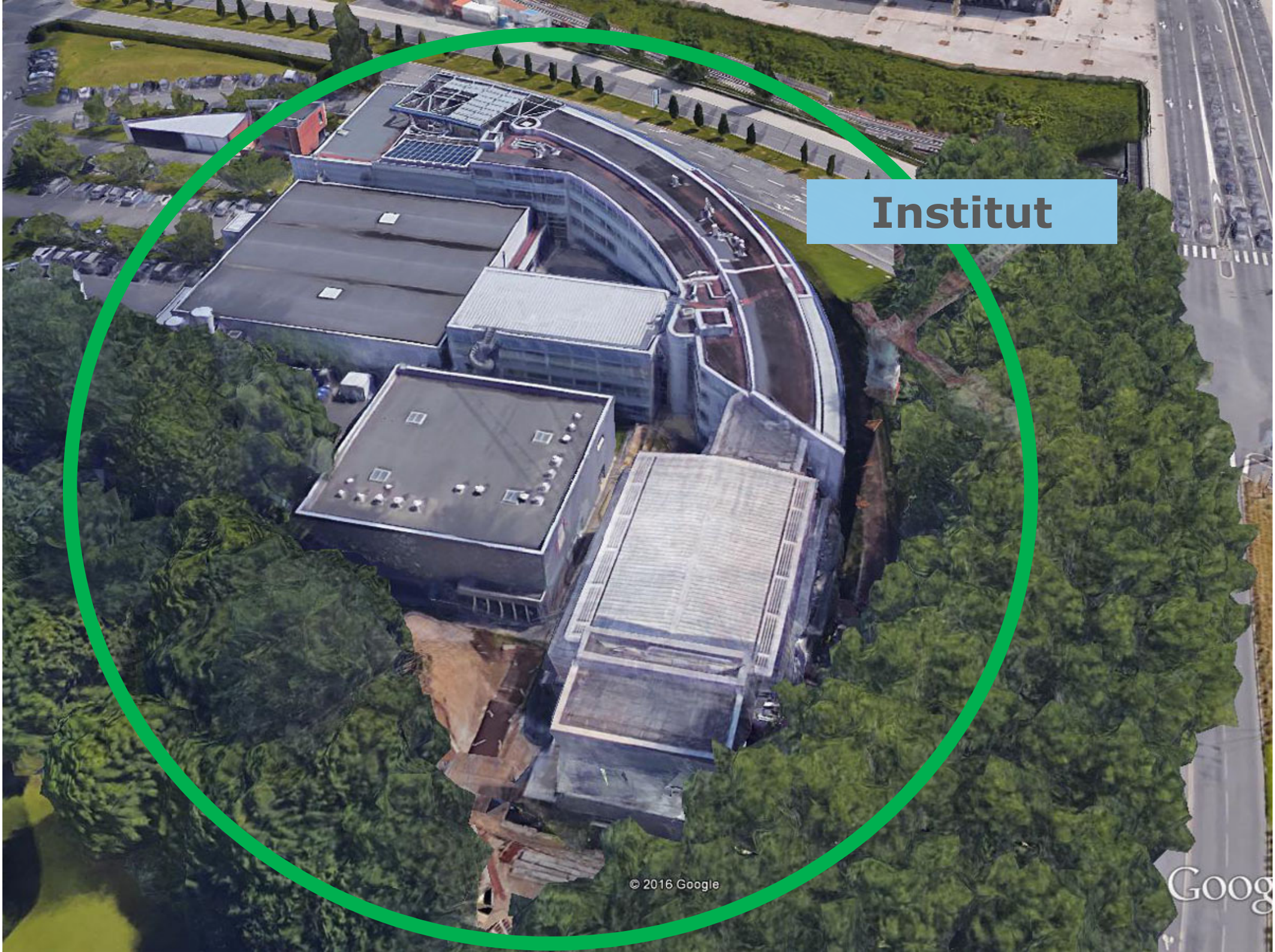
...PARTICULARITÉS SSI CAMPUS
On n'est pas normal ?

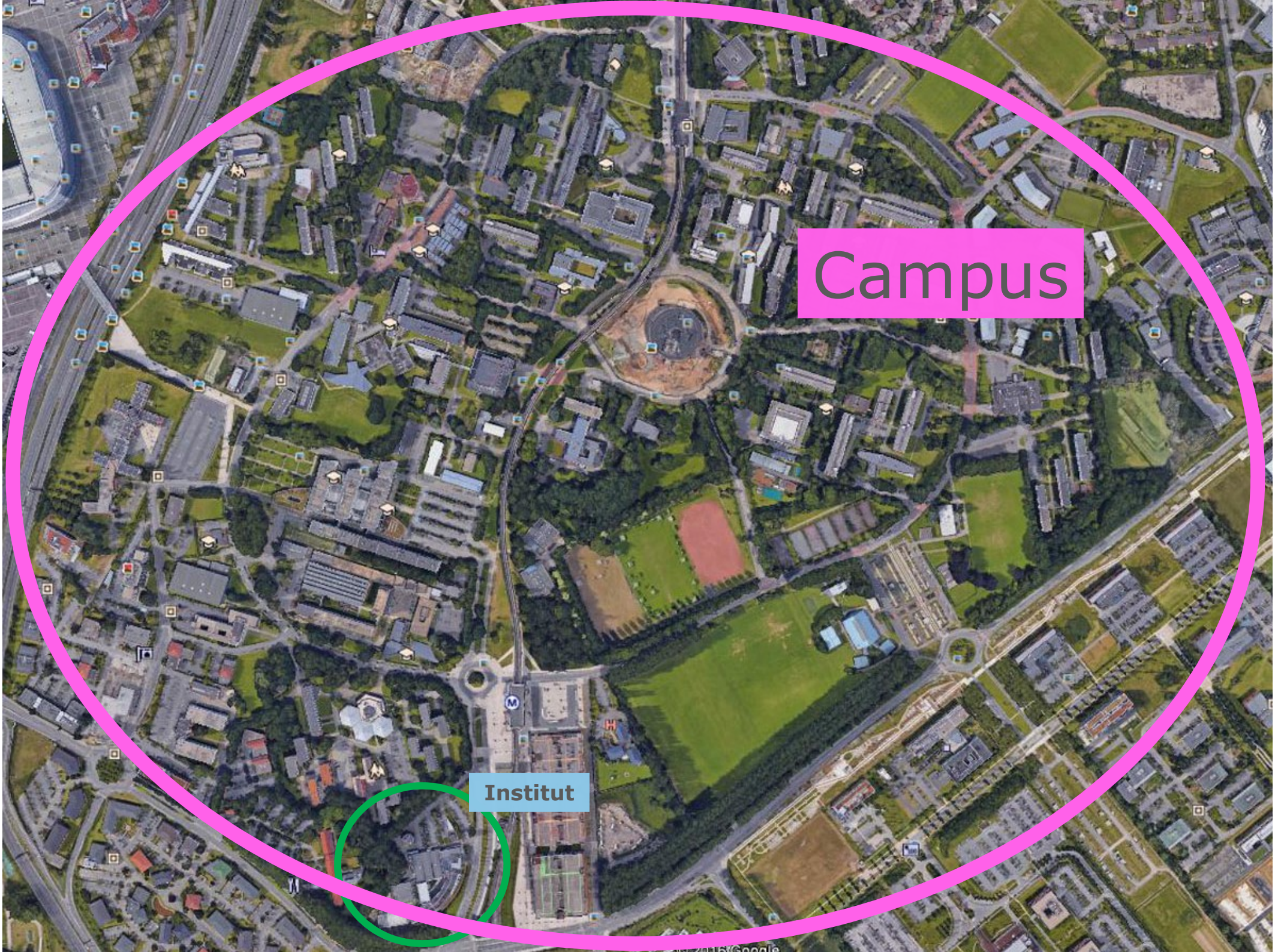
3) La gouvernance a bien d'autres chats à fouetter

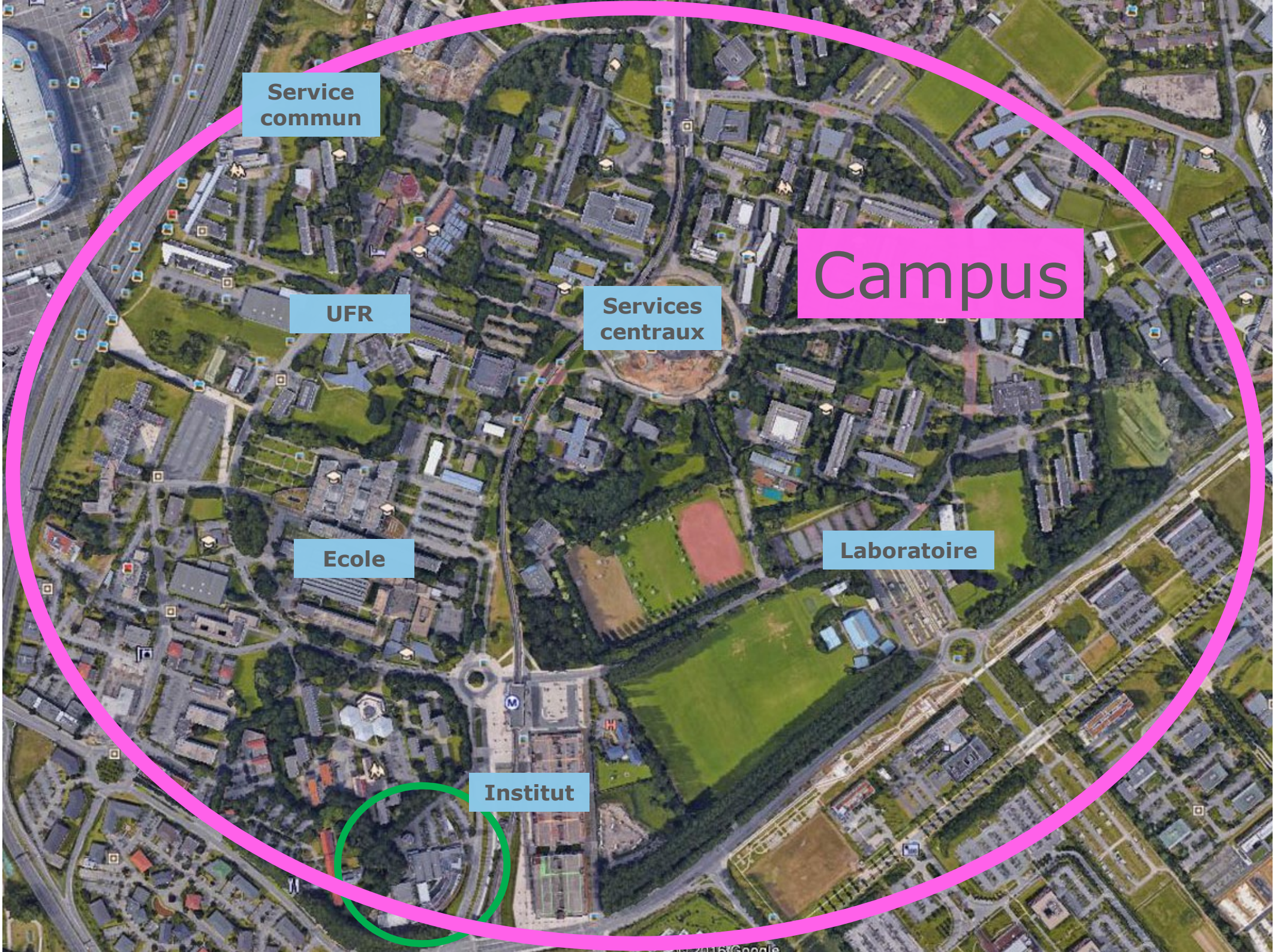
- **risques professionnels,**
- **des dizaines de bâtiments à sécuriser,**
- **stationnements sauvages,**
- **opposants aux expérimentations animales (y compris sur les chats),**
- **fusions (d'Universités) et autres menaces,**
- **etc...**

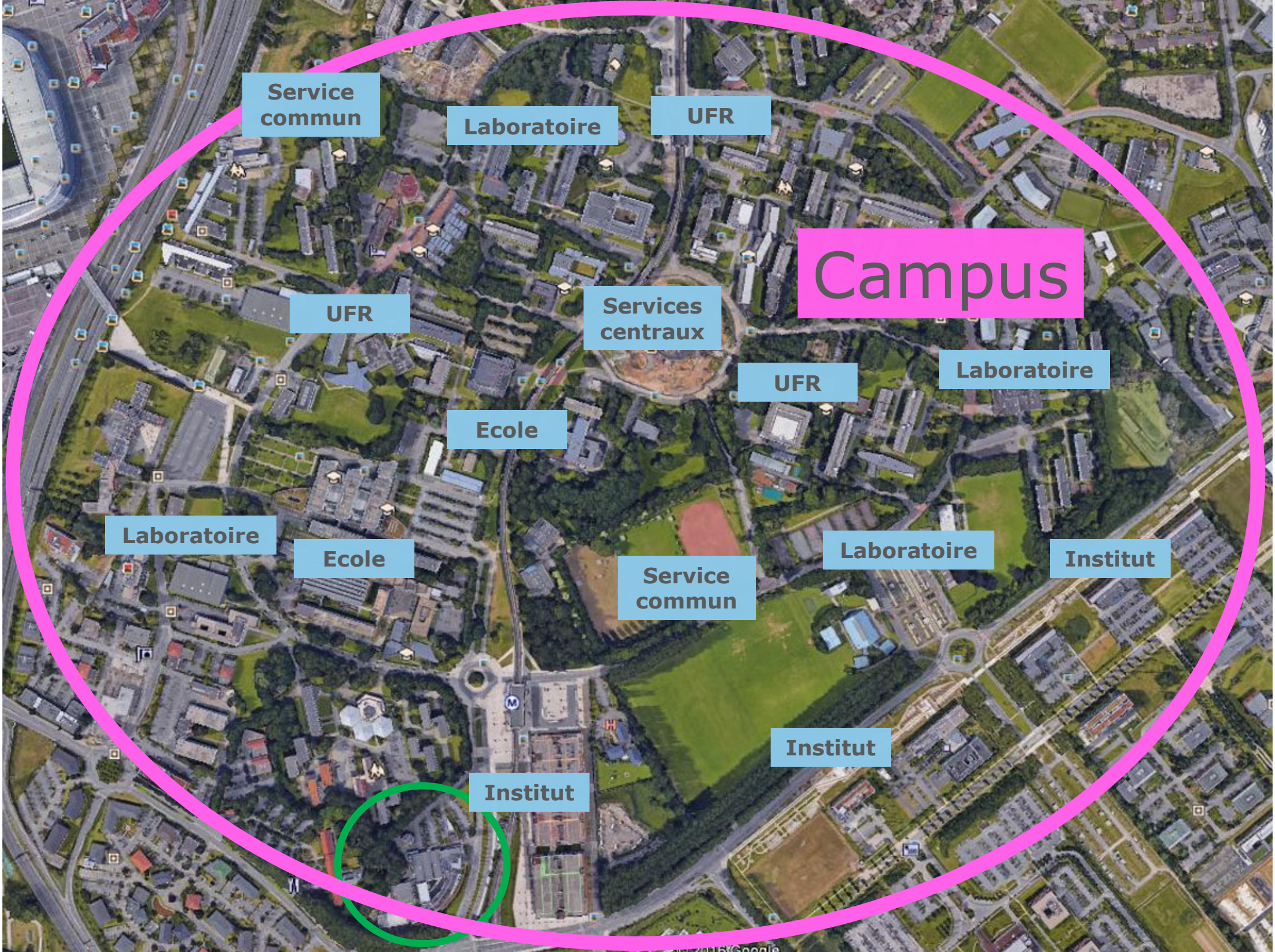
4) C'est plein de petits jeunes (les étudiants) qui présentent un gros turn-over (*-cent fois sur le métier...*)

5) Les châtiments corporels sont interdits ;-)


Institut
© 2016 Google


Campus
Institut


Service commun
Campus
UFR
Services centraux
Ecole
Laboratoire
Institut


Campus
Service commun
Laboratoire
UFR
UFR
Services centraux
UFR
Laboratoire
Ecole
Laboratoire
Ecole
Service commun
Laboratoire
Institut
Institut
Institut


Service commun
Laboratoire
UFR
Campus
UFR
Services centraux
Laboratoire
Un campus universitaire se gère plus comme une ville de taille moyenne que comme une Entreprise
Laboratoire
Ecole
Laboratoire
Institut
Service commun
Institut
Institut

RIEN D'IMPOSSIBLE…
On va y arriver (si, si)

1) Derrière l'apparent chaos, repérer les zones de stabilité

- **un réseau du Campus géré en central,**
- **des matériels et logiciels relativement peu diversifiés (marchés, groupements d'achat),**
- **un profil assez homogène des gestionnaires de parc et des administrateurs système (ITRF BAP-E, au courant des bonnes pratiques, peu de « volontaires + ou - désignés d'office »),**
- **des mesures de protection « standardisées » (PSSI-E).**

RIEN D'IMPOSSIBLE…
On va y arriver (si, si)

2) Relativiser le risque :

- un risque assez faible (importance de la menace toute relative, conséquences rarement "mortelles" pour l'Etablissement)
  - ➢ exceptions : PPST, ZRR

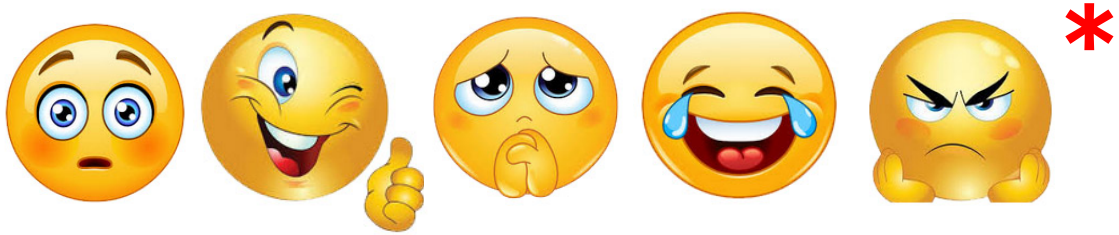
➔ incidents basiques (*et assez faciles à réduire*) : perte de données (*sauvegarder*), phishing (*sensibiliser, filtrer*), défiguration de sites WEB (*mettre à jour*), virus, malware, trojan (*mettre à jour, sécuriser les postes de travail*), peer to peer (*sermonner, bloquer*), etc…

Y a rien qui va mal !

…RIEN D'IMPOSSIBLE…

On va y arriver (si, si)

3) Avoir un bon RSSI



*

- qui connaît bien le milieu (profil « senior »),
- qui est bien connu du milieu,
- qui a la patience d'argumenter (logiquement, bien évidemment),
- qui évite dogmatisme et mails sentencieux,
- qui sait malgré tout décider,
- qui ne craint pas (ou plus) pour sa carrière…

* : Rayer les mentions inutiles

…RIEN D'IMPOSSIBLE
On va y arriver (si, si)

4) Réunir quelques conditions :

- **un RSSI en bons termes avec VP TIC, DSI, experts SSI,**
- **un maximum d'ETP dédiés à la SSI (maximum >= 1),**
- **un bon réseau de Correspondants SSI dans les composantes/labo,**
- **dans le cas des UMR, des exigences de sécurité pas trop différentes, ou des responsabilités définies par contrat (ex : CNRS ➔ priorité à la PSSI de l'Université),**
- **des bénévoles sur certains projets (mais pas toujours facile d'exiger quelque chose d'un bénévole, ni de son supérieur hiérarchique),**
- **du pragmatisme : démarrer en priorité les projets qui concernent un maximum de monde ou de ressources, et qui ne coutent pas cher.**

ET ALORS, A LILLE 1, ÇA DONNE QUOI ?...
y a pire (si, si)

Quelques projets aboutis (ou presque) :

- **règlement d'usage du SI (ça fait un bon moment...),**
- **adoption de la PSSI-E 2014,**
- **campagnes de sensibilisation au phishing,**
- **amélioration du compartimentage du réseau,**
- **sensibilisation à la sécurité des objets connectés (pan dans le climatiseur !),**
- **recommandations de sécurisation des MFP,**
- **charte Administrateur de Systèmes Informatiques (diffusée aux admins et aux responsables),**
- **sécurité des sites WEB (recommandations, cartographie),**
- **outil de scan de sites WEB (Acunetix).**

ET ALORS, A LILLE 1, ÇA DONNE QUOI ?...
y a pire (si, si)

Campagne de sensibilisation au phishing (09/2016)

Sujet : [ACT] Problème sur votre compte albert.duchmoll@univ-lille1.fr

Date : Thu, 22 Sep 2016 08:23:58 +0200

De : admin@serveur.univ-lille1.org

Pour : albert.duchmoll@univ-lille1.fr

Bonjour albert.duchmoll@univ-lille1.fr,

Un probleme a ete detecte avec votre compte de mail albert.duchmoll@univ-lille1.fr et vous devez reactiver le compte.

Pour effectuer l'action, cliquez sur le lien suivant et entrer les donnees :

serveur.univ-lille1.fr

Merci.

Le Service des Usages Numeriques de univ-lille1.fr

usage_numeric@univ-lille1.fr

03 20 33 99 99

http://assistance.univ-lille1.fr/

ET ALORS, A LILLE 1, ÇA DONNE QUOI ?...
y a pire (si, si)

Campagne de sensibilisation au phishing (09/2016)

Sujet : [ACT] Problème sur votre compte albert.duchmoll@univ-lille1.fr

Date : Thu, 22 Sep 2016 08:23:58 +0200

De : admin@serveur.univ-lille1.org

Pour : albert.duchmoll@univ-lille1.fr

Bonjour albert.duchmoll@univ-lille1.fr,

Un probleme a ete detecte avec votre compte de mail albert.duchmoll@univ-lille1.fr et vous devez reactiver le compte.

Pour effectuer l'action, cliquez sur le lien suivant et entrer les donnees :

href='http://serveur.univ-lille1.org/cas/login?ticket=noVZUqTdJQ45o8ABmpqz3Wh8kdyWpfYW~AZER'

Merci.

Le Service des Usages Numeriques de univ-lille1.fr

usage_numeric@univ-lille1.fr

03 20 33 99 99

http://assistance.univ-lille1.fr/

ET ALORS, A LILLE 1, ÇA DONNE QUOI ?...
y a pire (si, si)

Campagne de sensibilisation au phishing (09/2016)

ET ALORS, A LILLE 1, ÇA DONNE QUOI ?...
y a pire (si, si)

Campagne de sensibilisation au phishing (09/2016)

- **mails envoyés : 3949 (tous les personnels)**
- **mails ayant été relevés par un client de messagerie (pas nécessairement lus) : 3336**
- **accès au site WEB : 400**
- **utilisateurs ayant communiqué leur mot de passe : 133**
- **Utilisateurs ayant signalé le phishing : environ 300 (quantité appréciable)**

On recommencera !

ET ALORS, A LILLE 1, ÇA DONNE QUOI ?...
y a pire (si, si)

Pistes d'amélioration (pour ne pas dire : qu'est ce qui ne fonctionne pas ?) :

- **Amélioration de la prise en compte des aspects juridico-légaux (RGS, eIDAS, procédures de dépôt de plainte, ...),**
- **prise en compte de la SSI à chaque étape de la vie d'un projet,**
- **documentations « guides utilisateurs » ,**
- **communication institutionnelles (site WEB),**

- **outils de mesures, d'audit, de centralisation et d'analyse des logs,**
- **budget spécifique SSI (lettre au père Noël).**

CONCLUSION
y a pire (si, si)

- Augmentation de la sensibilité à la sécurité ; liberté totale n'est plus l'idée dominante ; la perception de la SI est passé de « [illegible] aucune importance » à « [illegible] ennuyeux, mais important »
- Sécurisation tous azimuts, pas seulement technique
- Mais importance de la sensibilisation : I had a dream© : que la SSI soit un réflexe pour tous
- Confiance indispensable (fragile)
- Importance des relais, i.e. des admins
- RSSI = « evangelist » ➔ porter la bonne parole
- Etre conscient des limites du bénévolat
- Université de Lille : comment gérer le changement d'échelle ?

DES QUESTIONS ?

Vite, on est en retard