Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA DÉFENSE

Sécurité Physique / Sécurité Logique

Décembre 2007

DGA

DÉLÉGATION GÉNÉRALE POUR L'ARMEMENT

La SSI

- Selon ISO 17799 :
  - La sécurité de l'information est assurée par la mise en œuvre de mesures adaptées, qui regroupent des règles, des processus, des procédures, des structures organisationnelles, et des fonctions matérielles et logicielles.

- C'est un ensemble cohérent de mesures techniques / non techniques qui permet d'assurer un niveau de sécurité satisfaisant

Définition

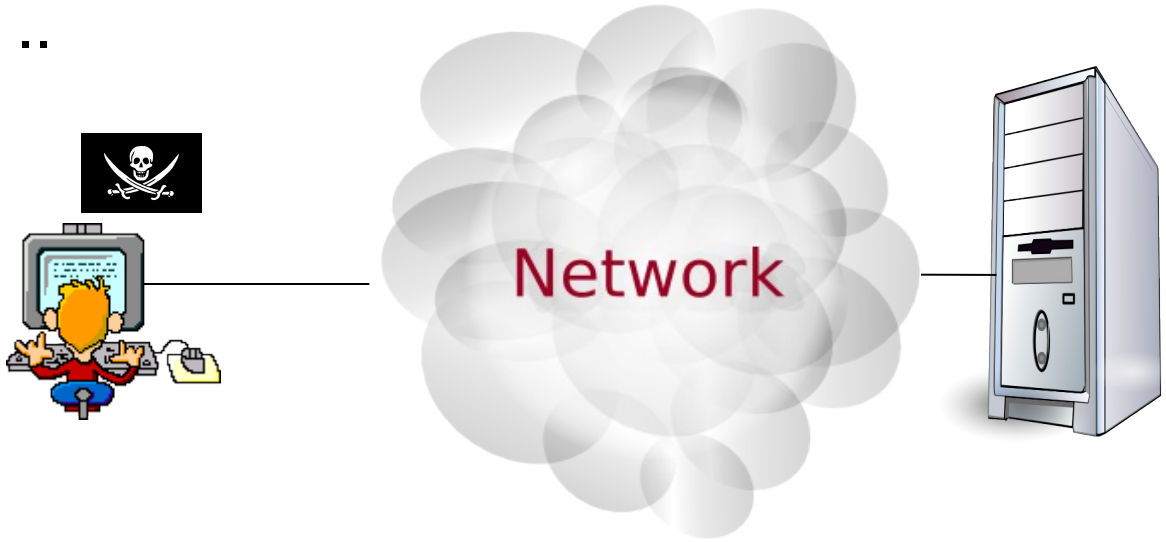
- Dans cette présentation, on appelera attaque logique toute exploitation des vulnérabilités des fonctions logicielles
- Dans les attaques physiques on inclut :
  - Les attaques sur l'environnement : coupure électrique, de climatisation,
  - Les attaques électroniques : brouillage, impulsions electromagnétiques
  - Les attaques matérielles : destruction physique, incendie, ...

Le point de vue de l'attaquant

- L'attaquant définit sa cible et ses objectifs en :
  - Confidentialité : récupérer des informations
  - Intégrité : modifier des informations
  - Disponibilité : détruire des informations ou provoquer un déni de service
- Son but :
  - Atteindre sa cible et ses objectifs de la manière la plus simple, la plus rapide, la moins chère, la moins risquée

Exemple : Récupération de coordonnées bancaires

- Attaque logique :
  - Recherche de vulnérabilité réseau,
  - Cryptanalyse de communications,
  - Key loggers
  - ..

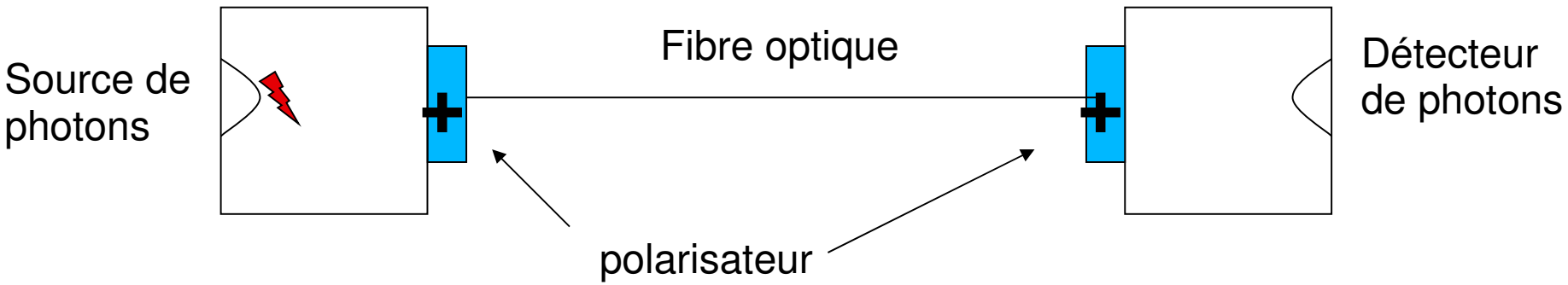


Exemple : Récupération de coordonnées bancaires

- Attaque physique :

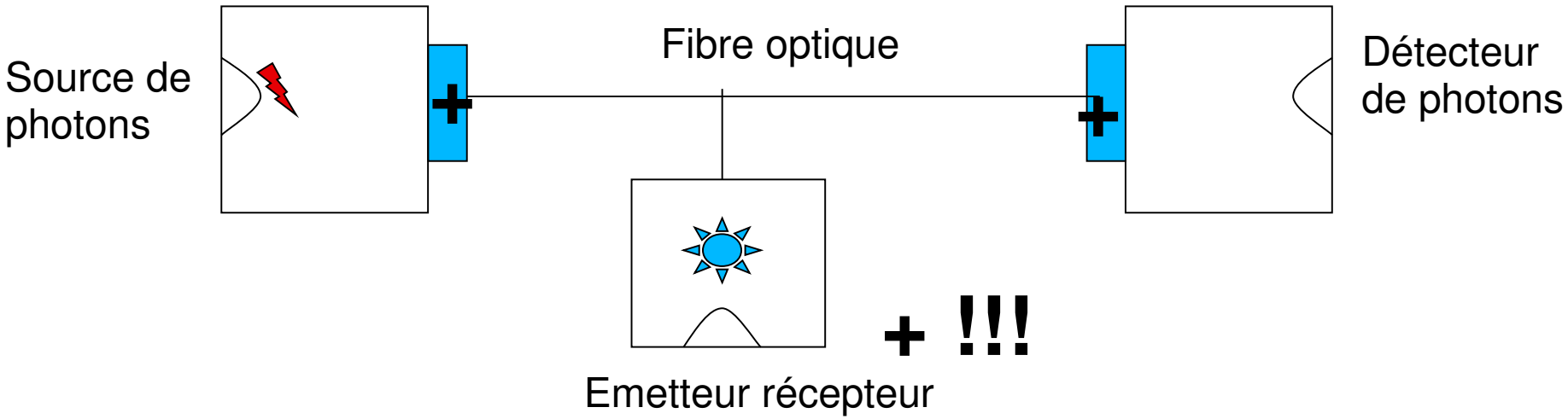
Exemple 2 : crypto quantique

- Cf exposé Adi Shamir durant C&esar :
  - Attaque logique théoriquement impossible (par principe, toute attaque est détectée)



  - Hypothèse : les polarisateurs sont positionnés (mécaniquement) avant l'émission du photon

Exemple 2 : crypto quantique



- On récupère la polarité du photon sans perturber les émissions licites

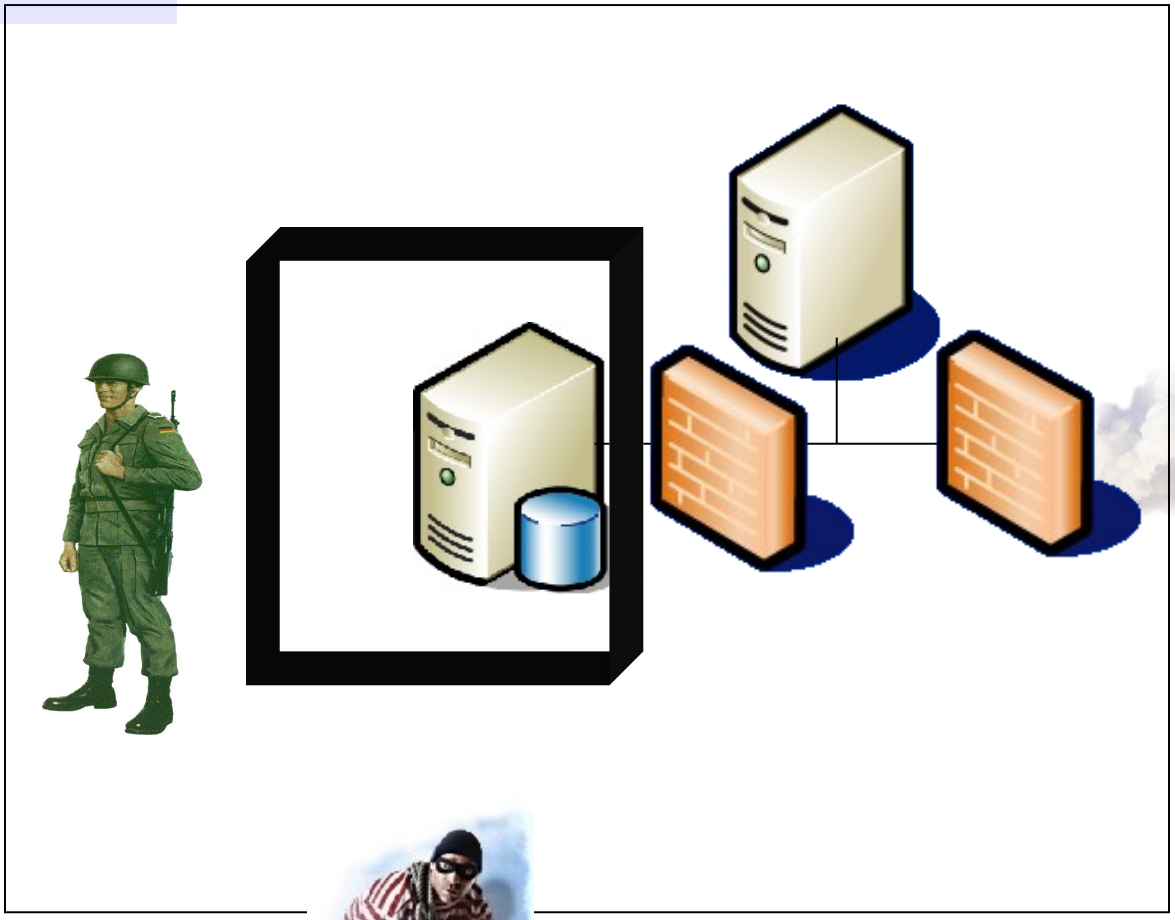
Au niveau Défense

- Que ce soit au niveau national ou OTAN, la sécurité repose de plus en plus sur la notion de défense en profondeur
- Exemple : II920 pour le traitement du Confidentiel Défense en France :
  - Entre les agresseurs potentiels et la cible, besoin d'au moins trois barrières ***physiques ou logiques***
- Voir aussi les travaux IATF sur ce même sujet

Défense en profondeur

- Origines :
  - Vauban
  - Sureté nucléaire
- Principes :
  - Ensemble de barrières autonomes, coopérantes
  - Barrières logiques, physiques ou humaines
  - Chaque barrière peut freiner l'adversaire, avertir, réagir, ...

Défense en profondeur



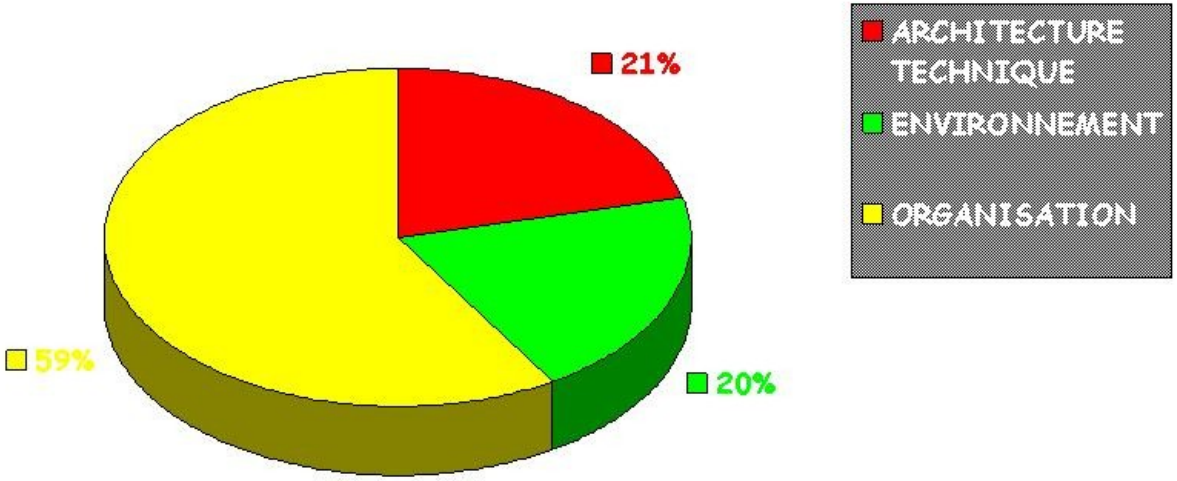
Analyse de risques

- Exemple : la méthode EBIOS
  - Les méthodes d'attaques physiques représentent un part importante des méthodes d 'attaques standard

    - Incendie
      - Dégâts des eaux
      - Destruction matériel
      - Pollution
      - Sinistre majeur
      - Défaillance de la climatisation
      - Perte alimentation électrique
      - Perte des moyens de télécommunication
      - IEM

    - Interception SPC
    - Vol de matériels
    - Vol de supports ou documents
    - Récupération de supports recyclés ou mis au rebut
    - Atteinte à la maintenabilité
    - Atteinte à la disponibilité du personnels

Quelques chiffres : retour d'expérience sur audits



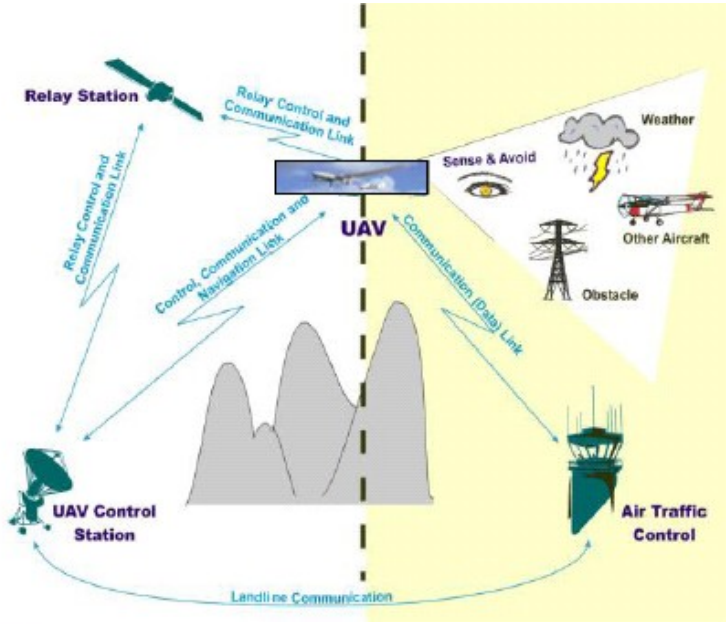
Exemple de scénario

Le contexte

- Le Hackistan a été attaqué par une coalition menée par Freedonia qui utilise un drone achetés à une grande puissance
- Objectif des rebelles retranchés dans les montagnes de Portscan : mettre le drone hors service

Première étape : collecte d'information source ouverte

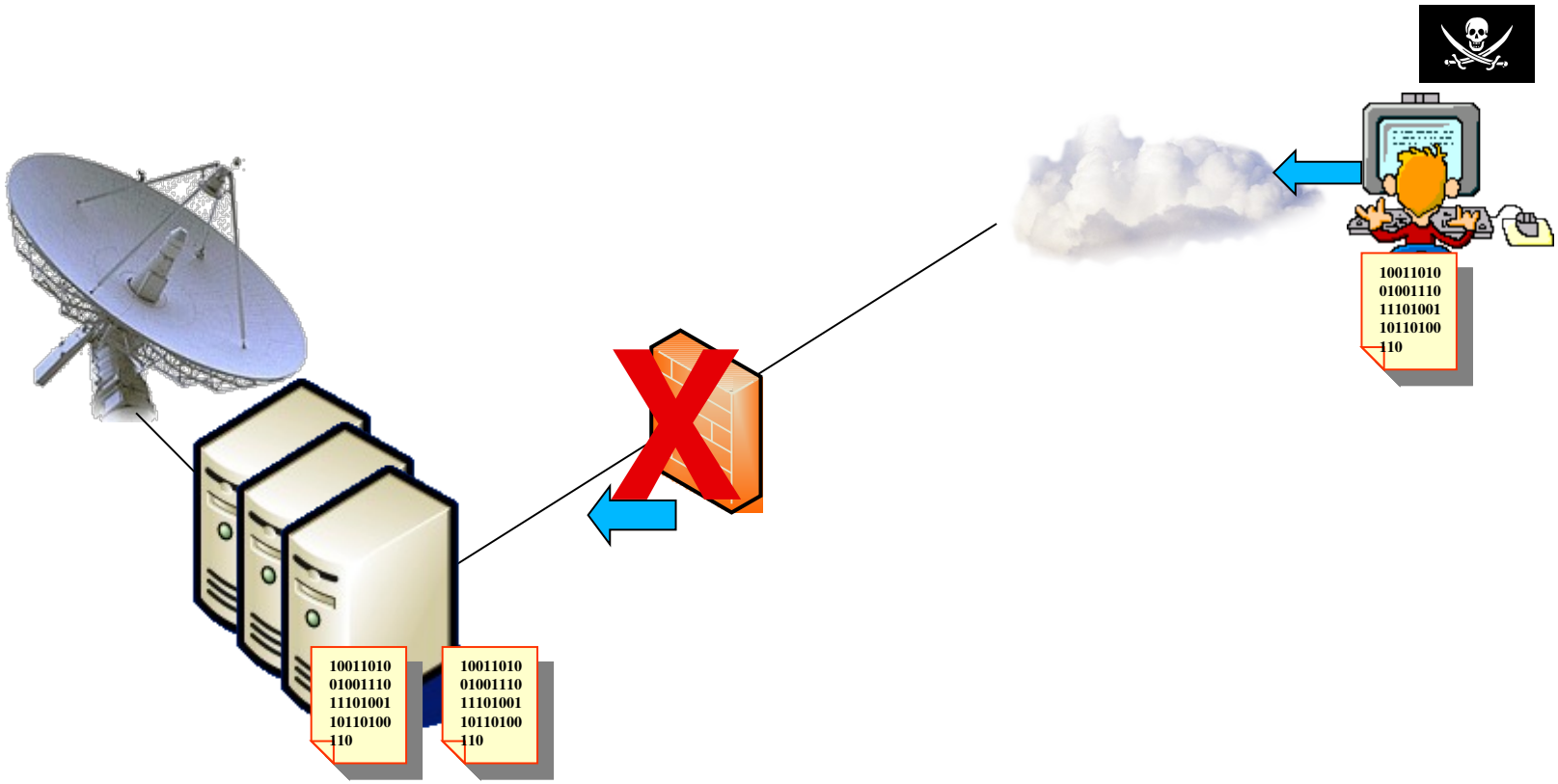
- Les drones ayant été largement diffusés sur le marché mondial, de nombreuses informations sont disponibles sur Internet



Analyse et détermination d'un objectif

- Après analyse de la documentation recueillie, deux équipes se mettent au travail
- Leur objectif, couper le moteur du drone en vol pour qu'il s'écrase
- Un moyen : modifier le logiciel de contrôle des moteurs, téléchargeable depuis le sol

1ère équipe


10011010
01001110
11101001
10110100
110
10011010
01001110
11101001
10110100
110
10011010
01001110
11101001
10110100
110

2ème équipe

- Récupère un moteur identique et donc le logiciel de pilotage
- Prépare une version piégée
- Profite du transport par camion du drone entre le port et sa base pour changer le calculateur par sa version piégée

Comparaison des deux approches

- Un point commun, l'analyse du logiciel, son désassemblage et sa modification

- Dans le premier cas :
  - une bonne configuration du firewall et des serveurs aurait pu empêcher complètement le déroulement de l'attaque
  - Il y a des traces de l'attaque dans le système
  - Beaucoup de difficultés : trouver le bon logiciel, le faire télécharger, etc

- Dans le second cas :
  - Une meilleure protection physique aurait suffit
  - Il faut profiter d'une situation opportuniste (transport)
  - Cette attaque réussit même si la passerelle réseau sensible / réseau public est d'une solidité à toute épreuve

Conclusion

- La sécurité physique et la sécurité logique sont complémentaires et doivent être mises en place de manière cohérente :
  - l'une sans l'autre ne sert à rien

- Il faut analyser tous les types de scénarios, y compris les scénarios mixtes :
  - A trop se focaliser sur la sécurité logique, on peut laisser des failles béantes qui rendent le système vulnérable par des attaquants même disposant de moyens limités