www.cnrs.fr

Sécurité des systèmes d'information pour la recherche

Vincent Mazenod
Expert CRSSI DR7

cyber guerre (2007)
Russie vs Estonie

cyber guerre (2007)
Russie vs Estonie

Russie (1) vs Estonie (0)

- suppression de la statue du soldat soviétique dans la capitale estonienne Tallinn
  - attaque commanditée par les Russes
    - équipe de Hackers patriotes
      - DDoS via botnet
    -
      - utilisation d'une armée de machines "zombies" dont l'attaquant a prélalablement pris le contrôle pour noyer un serveur sous un flux soutenu et continu de requête
      - le serveur ainsi surchargé par les requêtes "zombies" ne peut plus répondre aux requêtes "légitimes"
      - déni de service
  - l'Estonie est alors l'un des pays le plus dématérialisé au monde
    - le pays est entièrement paralysé (communication, banques, services) pendant plusieurs jours

cyberguerre (2010)
Stuxnet

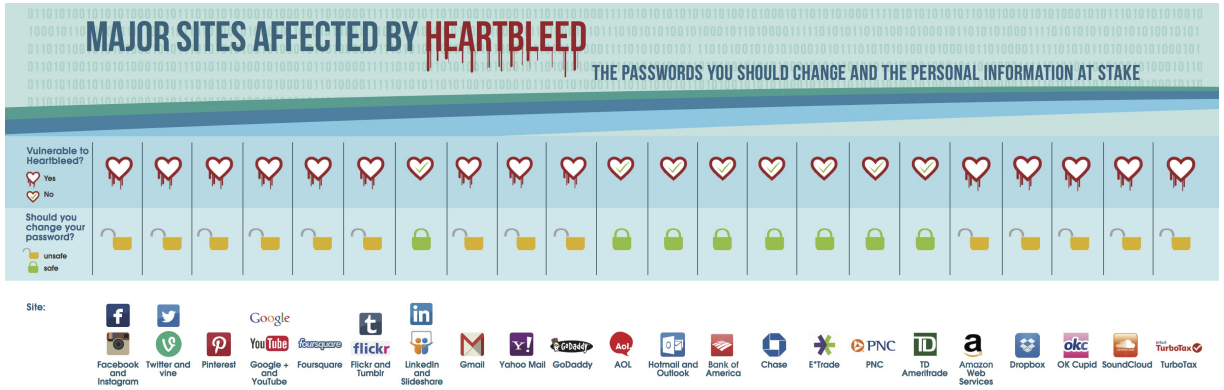
Stuxnet

- silencieux : 1 an avant sa découverte par les éditeurs d'antivirus
- ciblé
  - peut reprogrammer des automates industriels Siemens utilisant le système de télégestion SCADA (Supervisory Control And Data Acquisition)
    - vise les systèmes de contrôle des turbines à vapeur tels que ceux utilisés à la centrale nucléaire de Bouchehr (Iran)
      - modification de la vitesse des centrifugeuses
- complexe & couteux
  - utilise 3 exploits Windows "zero day"
    - pour se propager via le réseau et via l'USB
      - "dernier mètre" accompli avec une clé infectée
  - 6 mois de développement / de 5 à 10 personnes
  - attribué à une collaboration USA / Israël
- efficace: 2 ans de retard estimé pour le programme nucléaire iranien

heartbleed

heartbleed

- Bruce Schneier la positionne à 11 sur une échelle de 1 à 10
- absence d'une vérification sur la longueur d'un tampon
- on ne sait pas qui savait?
- on ne sait pas qui a pu exploiter (en deux ans)?
- il faut
  - mettre à jour asap
  - révoquer et changer tous les certificats
  - changer tous les mots de passe ayant transité sur la machine
- touche beaucoup de services



- mais aussi beaucoup d'équipements :/

Shodan HQ

SHODAN
Search
EXPOSE ONLINE DEVICES.
WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.
TAKE A TOUR
FREE SIGN UP
Popular Search Queries: cisco-ios last-modified - Finds Cisco-IOS results that do not require any authentication ;-)

Shodan HQ

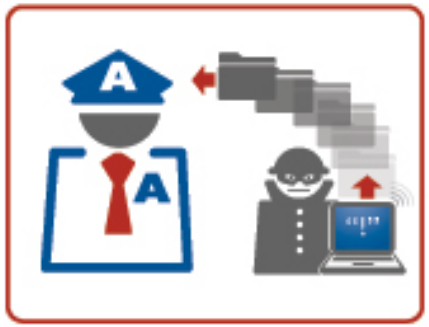
- découverte de l'Internet
  - en mode combinatoire /[0-255]\.[0-255]\.[0-255]\.[0-255]:\d/
  - en analysant les bannières de service
- prise en main rapide
  - search operators façon Google
    - Google-Fu sur tous les ports
    - exemple de Google-fu: intitle:"index of" "password.txt"
      - Google Hacking for Penetration Tester (by Johnny Long)
      - Google Hacking par HSC
    - exemple de requête Shodan: port:22 city:"Clermont-Ferrand"
      - Shodan for penetration testers
      - Les dernières requêtes pour l'inspiration

Absolute Computrace aka public LoJack

Computrace Agent is installed.

Computer is stolen.

Owner contacts local police and Absolute Software.



Absolute Theft Recovery Team forensically mines stolen computer for information.

Location of stolen computer is identified.

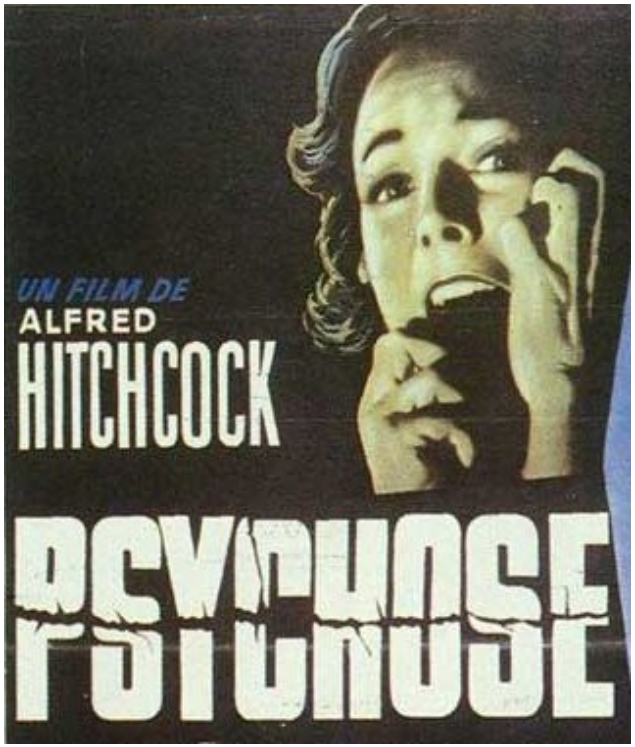
Absolute Theft Recovery Team works with local police agencies to recover stolen computer.

Absolute Computrace aka public LoJack

COMPUTRACE®
LOJACK® FOR LAPTOPS

- logiciel connu et officiel
  - ce n'est pas un virus
  - logiciel espion vendu comme tel
  - installer par les constructeurs via la partie inflashable du BIOS
    - découvert par hasard par un employé Kaspersky
- Computrace – Le mouchard universel présent sur les PC, Mac et appareils Android

c'est la ...



Alors que faire?

S'organiser!

quels enjeux pour la recherche

- protection des découvertes scientifiques et des brevets
- protection du matériel d'expérimentation scientifique
  - cohérence des résultats
  - sécurité des personnes
- données industrielles dans le cas de partenariat avec le privé
- toute information sensible et stratégique de l'établissement
- les locaux
- la population

Comment lutter efficacement contre la cyberguerre?
Comment surtout ne pas être ...

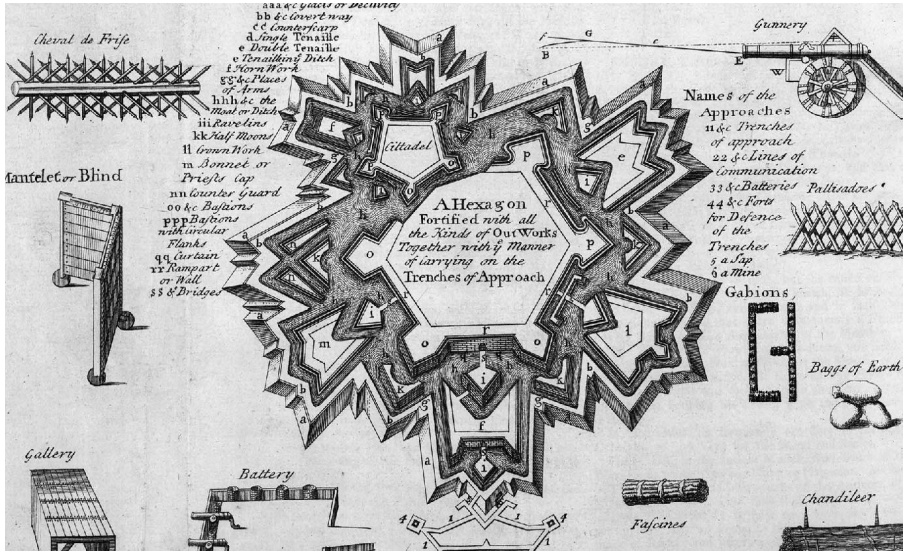
Le maillon faible!

... de la sécurité de la nation

La stratégie de la nation

La défense en profondeur

Sébastien Le Prestre de Vauban

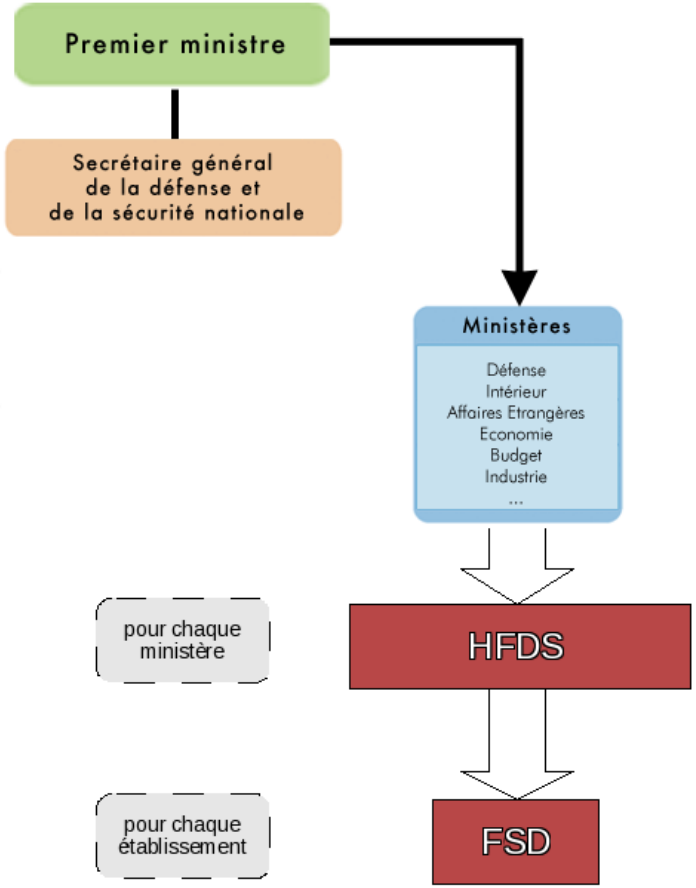


exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant particulier de sécurité est compromis ou défaillant

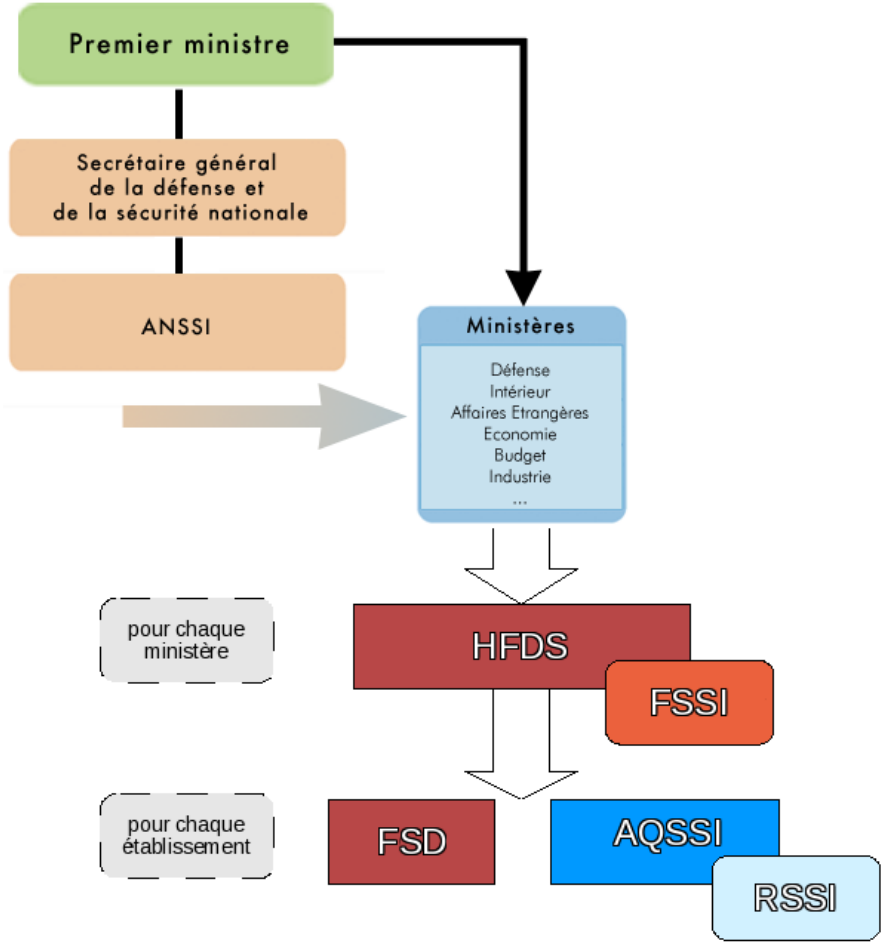
Stratégie de la défense en profondeur

- n'évite pas l'attaque
  - ralentit l'attaquant en lui opposant des difficultés multiples et variées
    - **chacun** est un maillon des chaînes fonctionnelles nationales de Sécurité Défense & SSI
      - **chacun** est donc responsable
        - de l'analyse des risques inhérents à son périmètre pour mieux les maîtriser
        - de l'anticipation & de la prévention des accidents et des actes de malveillance
        - de l'amélioration continuelle de la sécurisation de son périmètre
          - le risque 0 n'existe pas
          - la sécurité peut toujours être améliorée

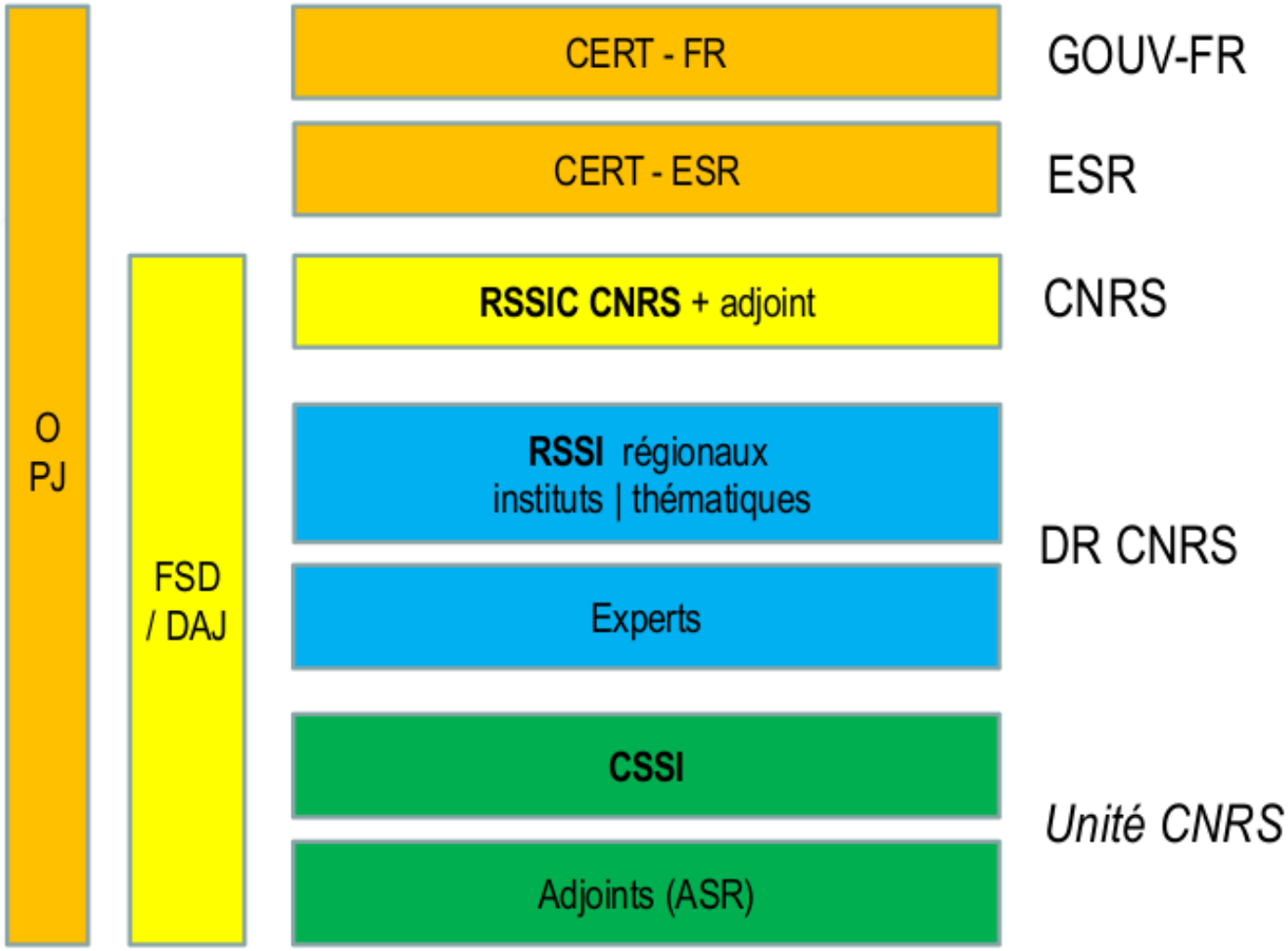
la chaîne Sécurité Défense



la chaîne SSI



Organisation au CNRS



Mise en oeuvre dans le monde de la recherche

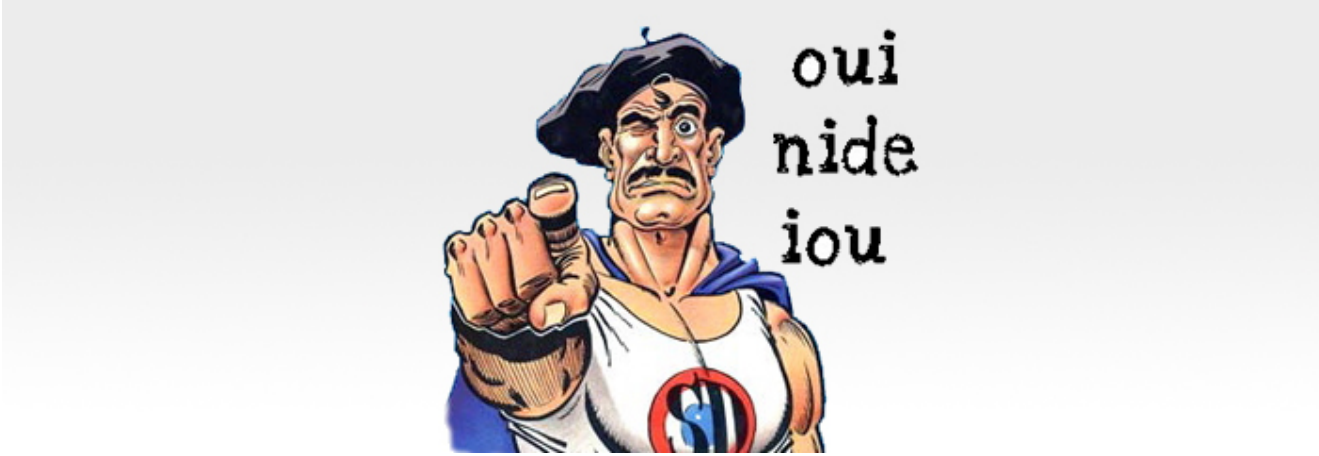
- la PPST : Protection du Patrimoine Scientifique et Technique
- C'est le rempart du monde de la recherche dans la chaîne de défense nationale
  - L'activité de recherche n'est pas un secteur d'activité d'importance vitale (SAIV) pour la nation
    - Mais elle participe largement aux technologies utilisées par les organismes d'importance vitale (OIV)
      - un laboratoire de recherche touchant directement une OIV sera probablement ZRR
- protection du « savoir » et « savoir faire »
- protection des personnes physiques (Conseils aux voyageurs sur diplomatie.gouv.fr)
- lutte contre le terrorisme
- non prolifération des armes de destruction massive

Mise en oeuvre au CNRS

- engagé dans la démarche SSI depuis 2007
- contexte particulier
  - éclatement géographique
  - hétérogénéité des domaines de recherche
  - démultiplication des partenariats avec d'autres instituts
- plusieurs chantiers en cours
  - PGSI (anciennement PSSI (Politique de sécurité des systèmes d'information))
    - règles simples (pas seulement informatiques)
    - adaptable au contexte (3 niveaux de séucrités)
  - chiffrement des portables avec TrueCrypt
  - guide des bonnes pratiques pour les administrateurs & les utilisateurs
  - gestion d'incidents
  - BYOD
  - défense active

n'oubliez pas que ...

- nous sommes tous en possession de données sensibles et à forte valeur ajoutée
- chacun est un rempart dans la défense en profondeur
- chacun est un maillon des chaînes Sécurité Défense et SSI
- gérer la sécurité de son périmètre c'est garder sa souveraineté technologique



Merci de votre attention!

... Des questions?