# NSA: le diable ou une agence de sécurité pour la démocratie?

**Virgil Gligor**
Carnegie Mellon University
Pittsburgh, PA 15213

**Swiss Cyber Risk Research Conference**
Swiss Tech Convention Center - EPFL
Lausanne, Switzerland
May 20, 2016

# Déclaration complète

1. Je n'ai eu:
   - *aucun soutien de la NSA,* recherche ou autre, directement ou indirectement, et
   - *que très peu de contacts* avec la direction de la NSA (direction, direction du développement, direction de la technologie) au cours des sept dernières années

   et *aucun* contact n'est prévu dans un proche avenir …

2. Je n'ai utilisé *que des informations publiques*
   - *aucune* autorisation de sécurité, *aucune* fuite ☺

3. Je *ne parle pas au nom* d'organisations avec lesquelles j'ai été en relation directe ou indirecte

   et *toutes les* opinions exprimées et les erreurs relèvent de *ma responsabilité*

# NSA: le diable ou une agence de sécurité pour la démocratie?

## Réponse: les deux

... pour certaines définitions (non religieuses) du diable et de la démocratie.

## Dans les grandes lignes

- Que fait un diable en cybersécurité et comment agit-il?
  Il établit une présence continue dans un réseau –
  ***ce qui n'est pas spécifique à la NSA***

- Trois dilemmes pour un monde interconnecté

- Solutions possibles: l'exemple de la ***NSA***

**Le diable** (en cybersécurité): un adversaire

Il établit une *présence continue* dans un réseau de protection, en exploitant

- *les coûts et les désagréments* d'une sécurité sur mesure et des systèmes de niche
- l'insécurité fondamentale des systèmes de commodité et des réseaux
- la faiblesse de la nature humaine; par ex. acheter, soudoyer et employer des méthodes de chantage (B3)

**Le diable** (en cybersécurité): un adversaire

Il établit une *présence continue* dans un réseau de protection, en exploitant

- *les coûts et les désagréments* d'une sécurité sur mesure et des systèmes de niche
- l'insécurité fondamentale des systèmes de commodité et des réseaux
- la faiblesse de la nature humaine; par ex. acheter, soudoyer et employer des méthodes de chantage (B3)

**La démocratie** (selon une conception occidentale):
un système politique où les citoyens

- choisissent/remplacent le gouvernement par des élections; pas de révolutions ni de coups d'Etat
- participent à la vie politique et civique => leurs droits doivent être protégés
- font confiance à l'Etat de droit, la loi devant être la même pour tous

***=> responsabilité publique du gouvernement***

**Le diable** (en cybersécurité): un adversaire

Il établit une *présence continue* dans un réseau de protection, en exploitant

- *les coûts et les désagréments* d'une sécurité sur mesure et des systèmes de niche
- l'insécurité fondamentale des systèmes de commodité et des réseaux
- la faiblesse de la nature humaine; par ex. acheter, soudoyer et employer des méthodes de chantage (B3)

**La démocratie** (selon une conception occidentale):
un système politique où les citoyens

- choisissent/remplacent le gouvernement par des élections; pas de révolutions ni de coups d'Etat
- participent à la vie politique et civique => leurs droits doivent être protégés
- font confiance à l'Etat de droit, la loi devant être la même pour tous

***=> responsabilité publique du gouvernement***

**Un service de renseignement étranger dans une démocratie:**

=> un diable pour les adversaires étrangers qui menacent ses institutions et son mode de vie

# Trois dilemmes

1) **pour une démocratie:** responsabilité *publique* des opérations *secrètes?*

- *pas de renseignement* sur les espions, les adversaires étrangers, les terroristes
- *pas de violation des droits privés* sous le sceau du secret

2) p**our un service de renseignement étranger:** comment viser des *adversaires étrangers, mais pas les citoyens dans le cyberespace?*
Qu'est-ce qu'un ciblage réussi?

- *test «caractère étranger»?*
- *test «but du renseignement»?*
- *test «ami ou ennemi»?*

3) **pour les citoyens:** comment avoir la certitude que leur propre service de renseignement étranger *ne les espionne pas?*
(amis et alliés: partageons-nous encore la même vision de la démocratie?)

# Dilemme 1: autre façon d'envisager la responsabilité?

**NSA's General Counsel** (*Georgetown University Law School*, 27 Feb 2013):

"*There is no perfect substitute for public transparency in a democracy.*"

"…, *we must largely rely on […] alternate means of accountability*"

# Dilemme 1: autre façon d'envisager la responsabilité?

## Executive

**DoD (1952) + ODNI (2004)**

UnderSec (Intelligence)

AsstSec (oversight)

Gen Counsel

IG (Congress appt)

Gen Counsel

IG (Congress appt)

Civil Liberties Protection Officer

## Legislative

**House & Senate (1952)**

**Committees:**
Intelligence
Judiciary
Armed Services
Homeland Security, etc.

## Judiciary

**11 Federal District Court Judges**
**FISC (Sup. Court. appt.) 1978**

## Independent

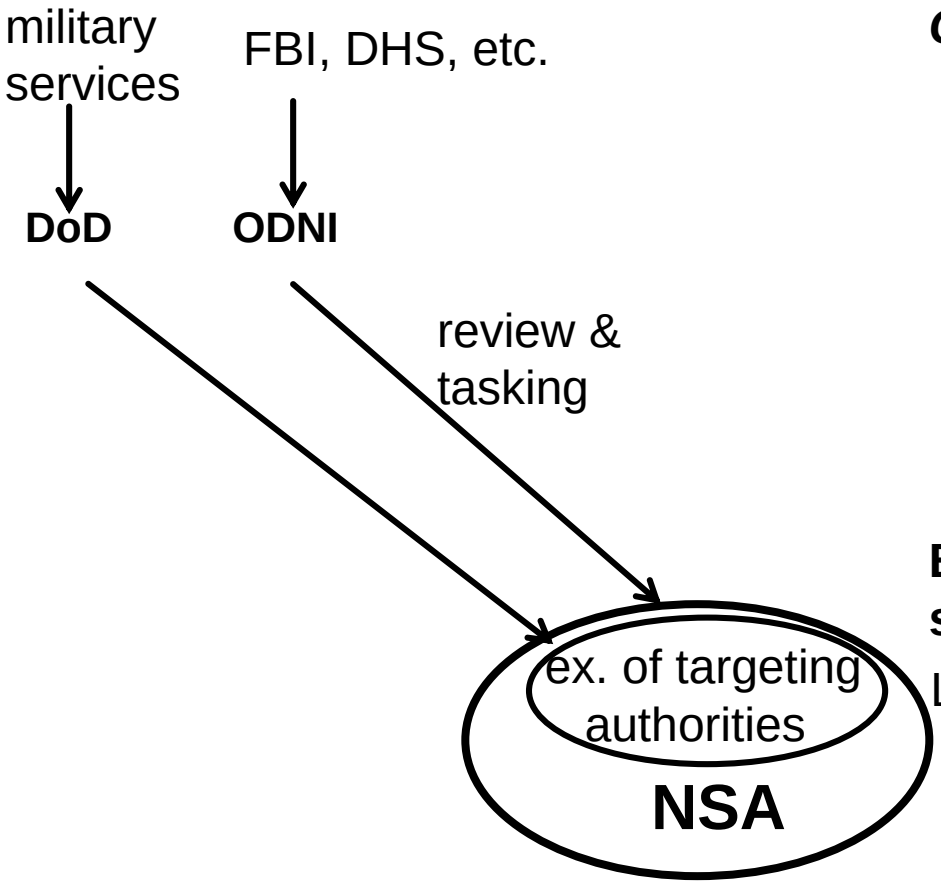
**Privacy & Civil Liberties Oversight Board (PCLOB)**

2004 – 2006 in the Executive Office?
2007 – 2012 --
2013 – New Board(Jan.)
2014 - Report on PA Section 215
2014 – Report on FISA Section 702
2016 - Assessment Report

## Internal

- compliance education, audit, access controls

# Dilemme 2: ciblage autorisé?




***Cible:* une personne *non US hors des USA***

*=> pas ciblée intentionnellement* ***:***

- n'importe qui aux *USA;* personne US *hors des USA*
  *(étranger venant aux USA -> personne US);*
- ciblage non entièrement national;
- pas de « ciblage inversé » depuis *l'extérieur des USA;*
- procédures de minimisation;
- pas de *violation du 4e amendement.*

**But: renseignement extérieur vise seulement des personnes non US?**

Les USA ont ratifié le PIDCP de 1966 (1992)

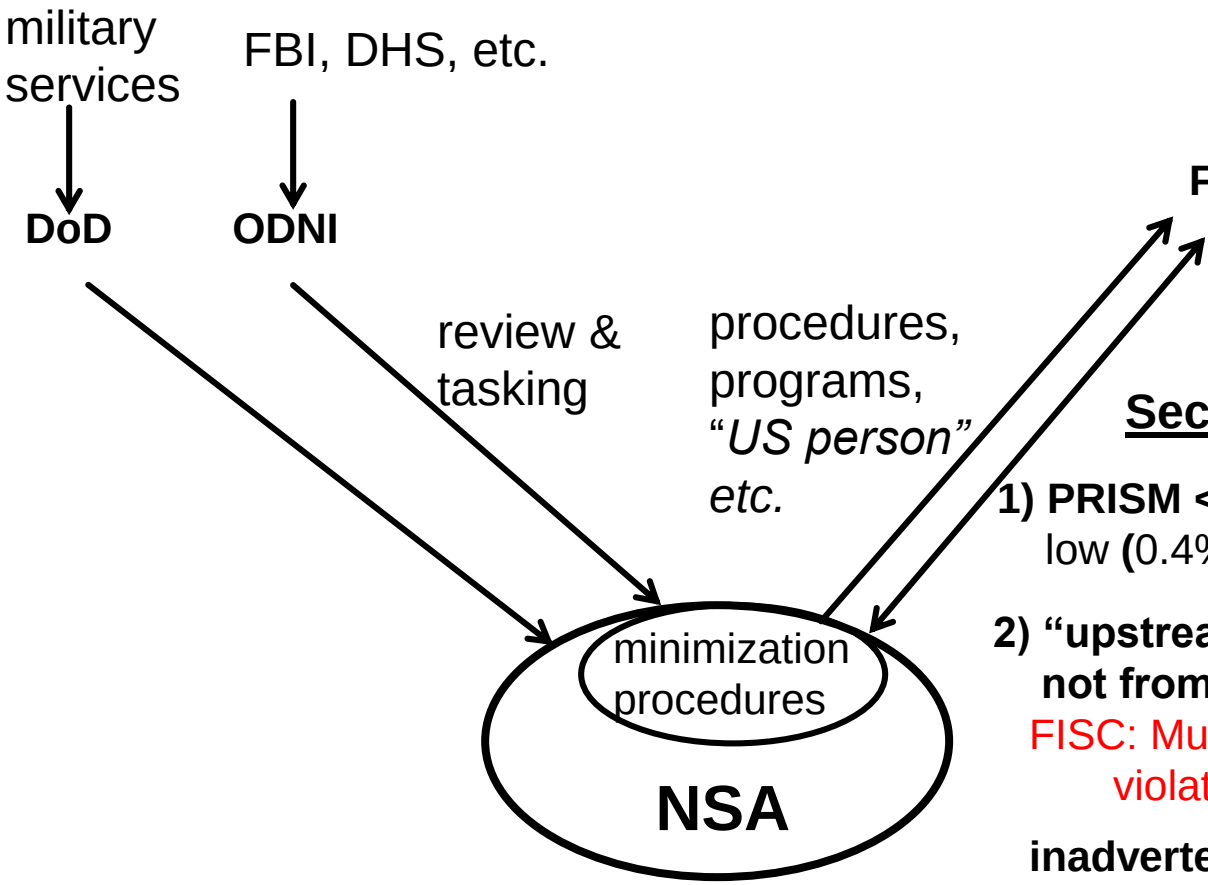
- Presidential Policy Directive 28 (2014)
  *limitée à la recherche d'informations*
  *mêmes « procédures de minimisation »*
  *qu'aux USA*

**1. Ex. Order 12333**
(outside US, 1981)

**2. Section 215 du Patriot Act**
(inside US, "call records," 2001)

**3. Section 702 FISA**
(inside US, amended 2008)

# Dilemme 2: ciblage correct?




**FISC – OKed NSA 2012 revisions**
ex. 198 US-person authorizations
9,500 US-person queries
89,138 overall targets (2013)

## Section 702 FISA

**1) PRISM <- specific ISP communication**
low (0.4% - 1.5%) error rate in 2013)

**2) "upstream" <- backbone communication**
**not from specific "to/from/about selector"**
FISC: Multi Communication Transactions
violated 4th Amendment (2008 – 2011)

**inadvertent collection; e.g., via MCT**
**~7 – 8K US persons, 97 – 140K can't tell**
no routine immediate deletion

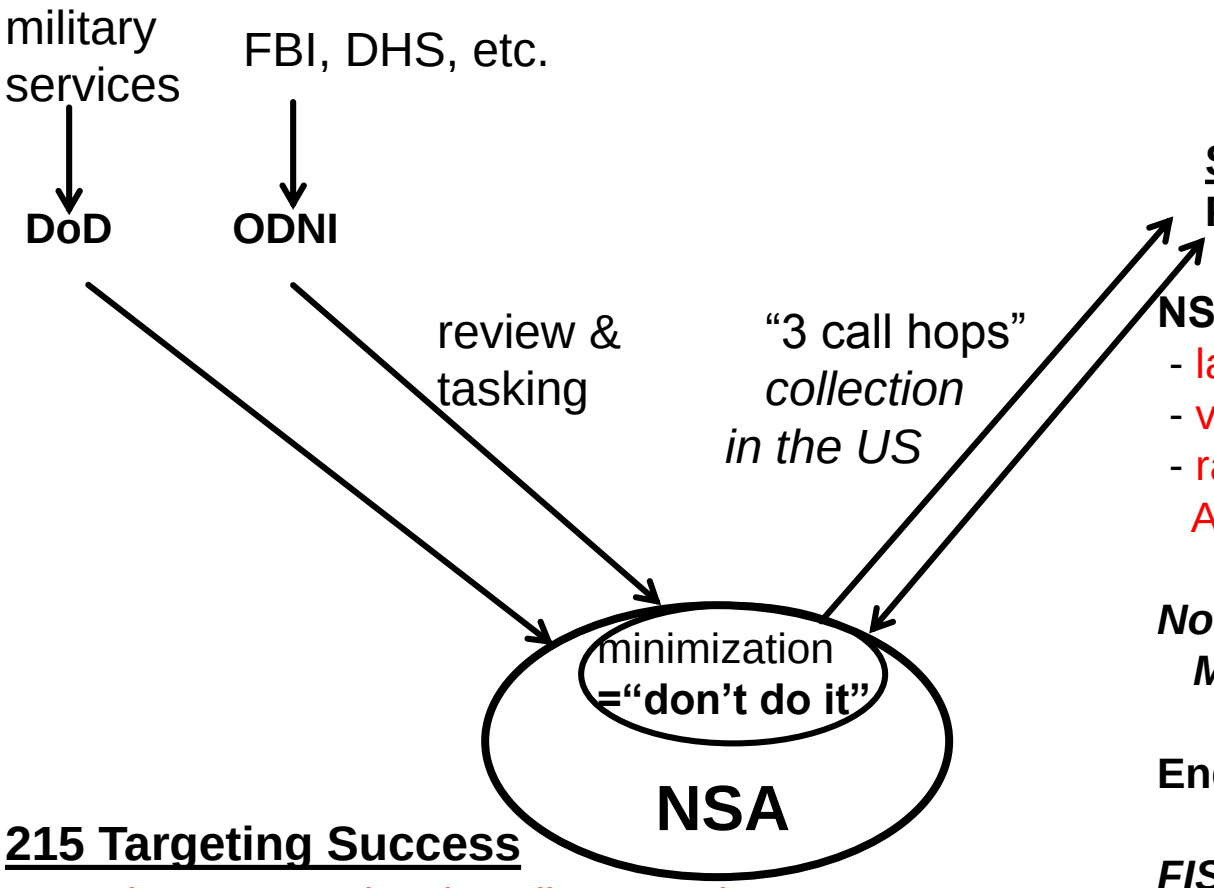
## 702 FISA Targeting Success

> 100 arrests on terrorism charges
e.g., 15 cases of US plots
40 cases of foreign country plots
weapons proliferation cases, etc.

## Executive Order 12333

**1) NSA internal audit found & reported**
13 willful violations in a decade

# Dilemme 2: ciblage correct?




**Section 215 of Patriot Act**
**FISC-reviewed every 3 months**

**NSA's interpretation of Section 215**
- lacks legal foundation
- violated ECPA 1986
- raised concerns under 1st & 4th Amendments to the Constitution

***No Evidence of Bad Faith or Misconduct by NSA***

**End bulk call-record collection**

***FISC lacks***
- opposing views & special advocates
- appellate review
- technical & outside legal assistance

**Declassification & Stat. Disclosures**

**215 Targeting Success**
- 0 unknown terrorist plots discovered
- 0 terrorist attacks discovered
- 1 arguably unknown terrorist found (no plot)
- additional leads re: contacts of suspects known to FBI
- avoid false positives and saves some FBI resources

# Dilemme 3: comment faire confiance?

## D'abord, commence par des fuites d'initiés et une presse libre ☺

*New York Times* (décembre 2005): "NSA eavesdrops without warrant"
*New York Times* (février 2006): "NSA collected 1.9T call records"
- Des changements substantiels de politique entre 2006 et 2012
- Les révélations de Snowden (juin 2013) ont accéléré le débat.
  Cependant, des fuites par bribes contribuent à la création de nombreux *mythes erronés* sur la NSA

## Ensuite, exige une forte responsabilité et une action législative

*Independent PCLOB* – most recommendations accepted by the US Government
e.g., June 1, 2015 Patriot Act (section 215) expired – no NSA bulk collection

*Legislative action; e.g., Email Privacy Act* (H.R. 699) – April 27, 2016
e.g., legal warrants needed for
- *email collection* from *service providers*
- obtaining a user's *geo-location data*

# Dilemme 3: comment faire confiance?

*"The Americans will always do the right thing … but only after they've exhausted all alternatives."*

-- *adaptation anonyme, en 1970, d'une citation de* Abba Eban, de 1967
(attribuée par erreur à Winston Churchill)

**Enfin, débattre jusqu'à l'épuisement de toutes les alternatives …**

e.g., Chilling Effects ... or Only Correlations?

- changes in Internet browsing behavior after Snowden's revelations
  e.g., Pew Research Center (2013), Matthews and Tucker (2015), Jonathon Penney (2016)

- self censorship in browsing re: topics on terrorism?
  OR change of search for "juicier" topics; e.g., Snowden's revelations? OR Both?

- US Federal Judge in rejects Wikimedia "upstream" lawsuit against NSA's (October 2015)
  … no evidence provided of NSA's Internet surveillance "at full throttle"

*Fact*: *91% of all targeted Internet communication is via PRISM*, not *"upstream"*

# Leçons tirées

**1. L'absence totale de transparence (par ex. ne jamais rien dire) a des conséquences prévisibles**

- conduit à des *mythes erronés;* plus d'une dizaine concernent la NSA
- conduit éventuellement à une perte de *confiance dans le gouvernement*

**2. Lors du réexamen des autorisations, les tribunaux doivent entendre un avocat du diable et pas seulement le promoteur de la cause (c'est-à-dire l'Agence de renseignement)**

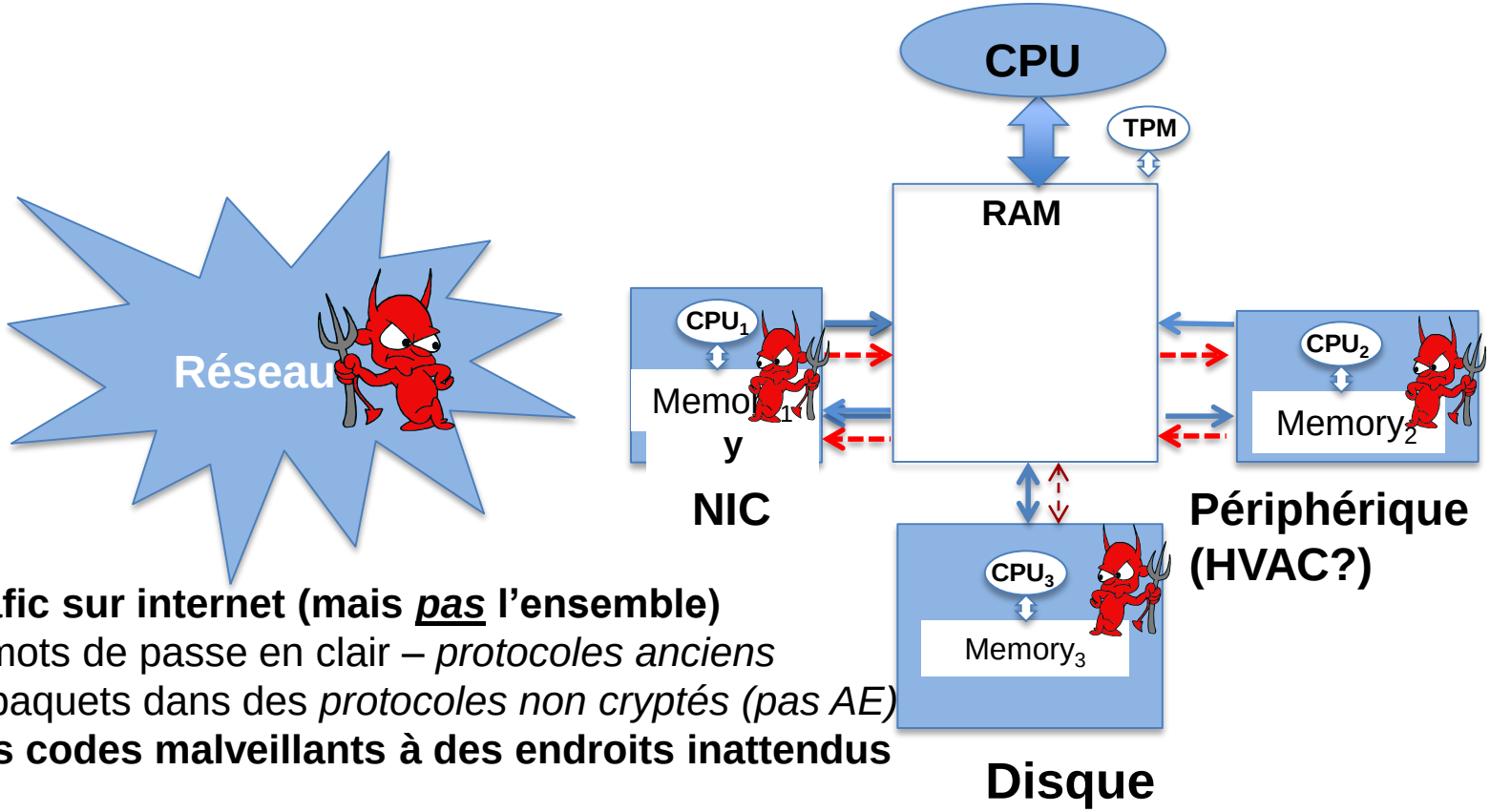
- les tribunaux doivent veiller à ne pas donner l'impression de rendre des décisions partiales

**3. Les lois et la politique gouvernementale doivent suivre la technologie**

- les autorisations de renseignement étranger doivent être réexaminées plus souvent qu'une fois tous les dix ans
- même avec leur savoir approfondi, les tribunaux ont besoin d'aide pour comprendre les nouvelles technologies

# Exemples:
# Que fait un diable en cybersécurité et comment agit-il?

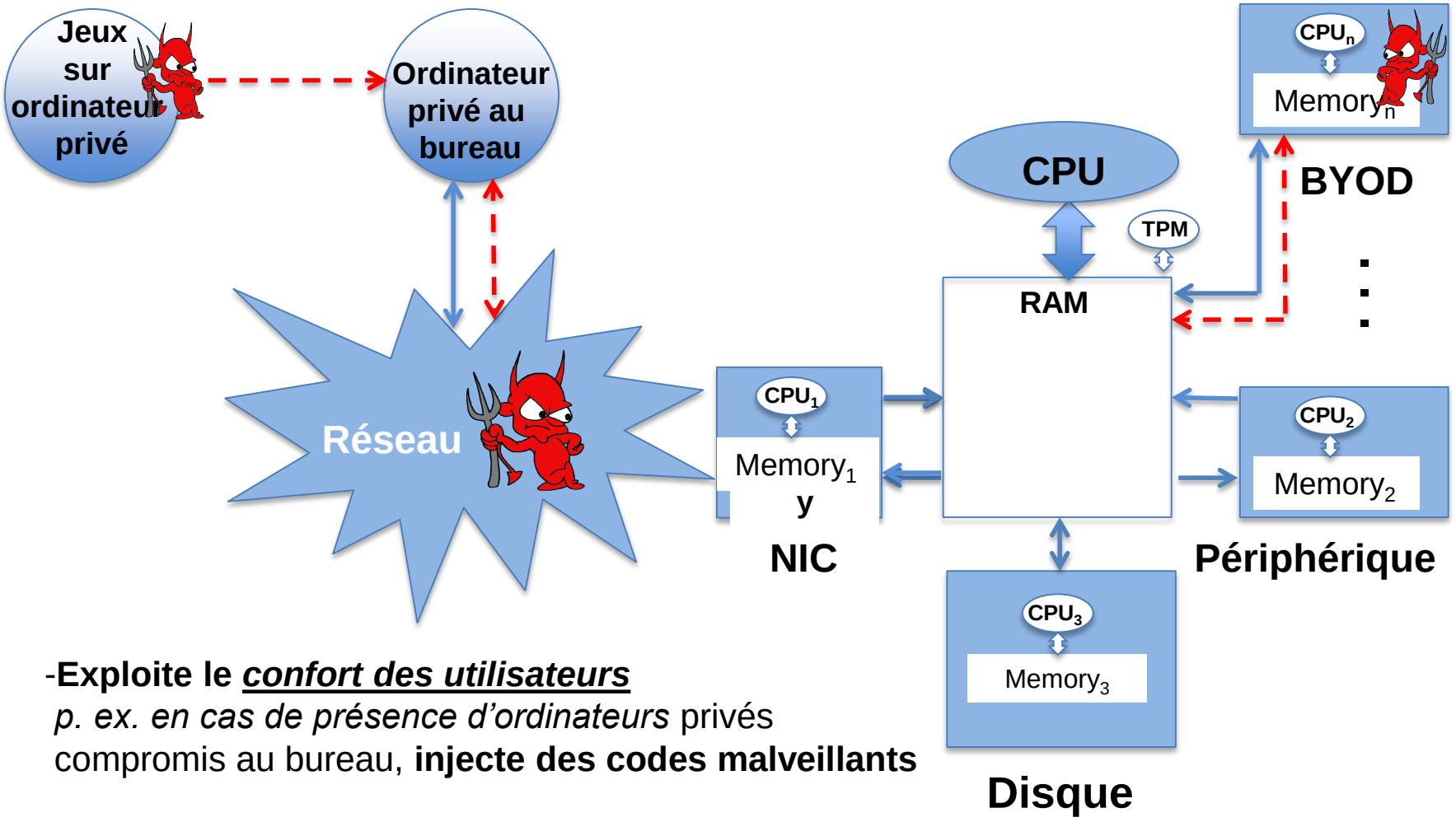
# Présence continue dans un réseau – pas un exemple de la pratique de la NSA




- **Surveille le trafic sur internet (mais *pas* l'ensemble)**
  - trouve des mots de passe en clair – *protocoles anciens*
  - injecte des paquets dans des *protocoles non cryptés (pas AE)*

  **et injecte des codes malveillants à des endroits inattendus**

# Présence continue dans un réseau – pas un exemple de la pratique de la NSA

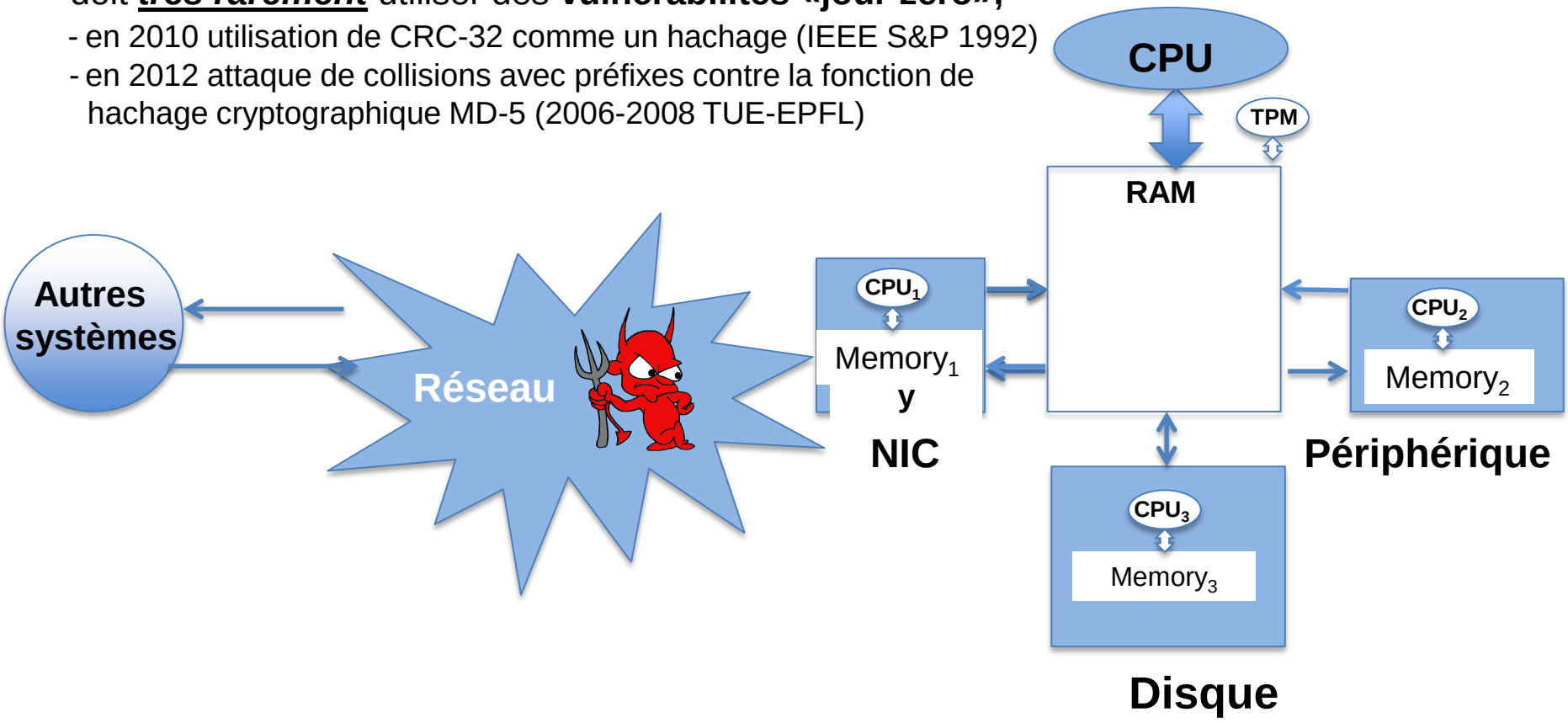



-**Exploite le *<u>confort des utilisateurs</u>***
*p. ex. en cas de présence d'ordinateurs* privés compromis au bureau, **injecte des codes malveillants**

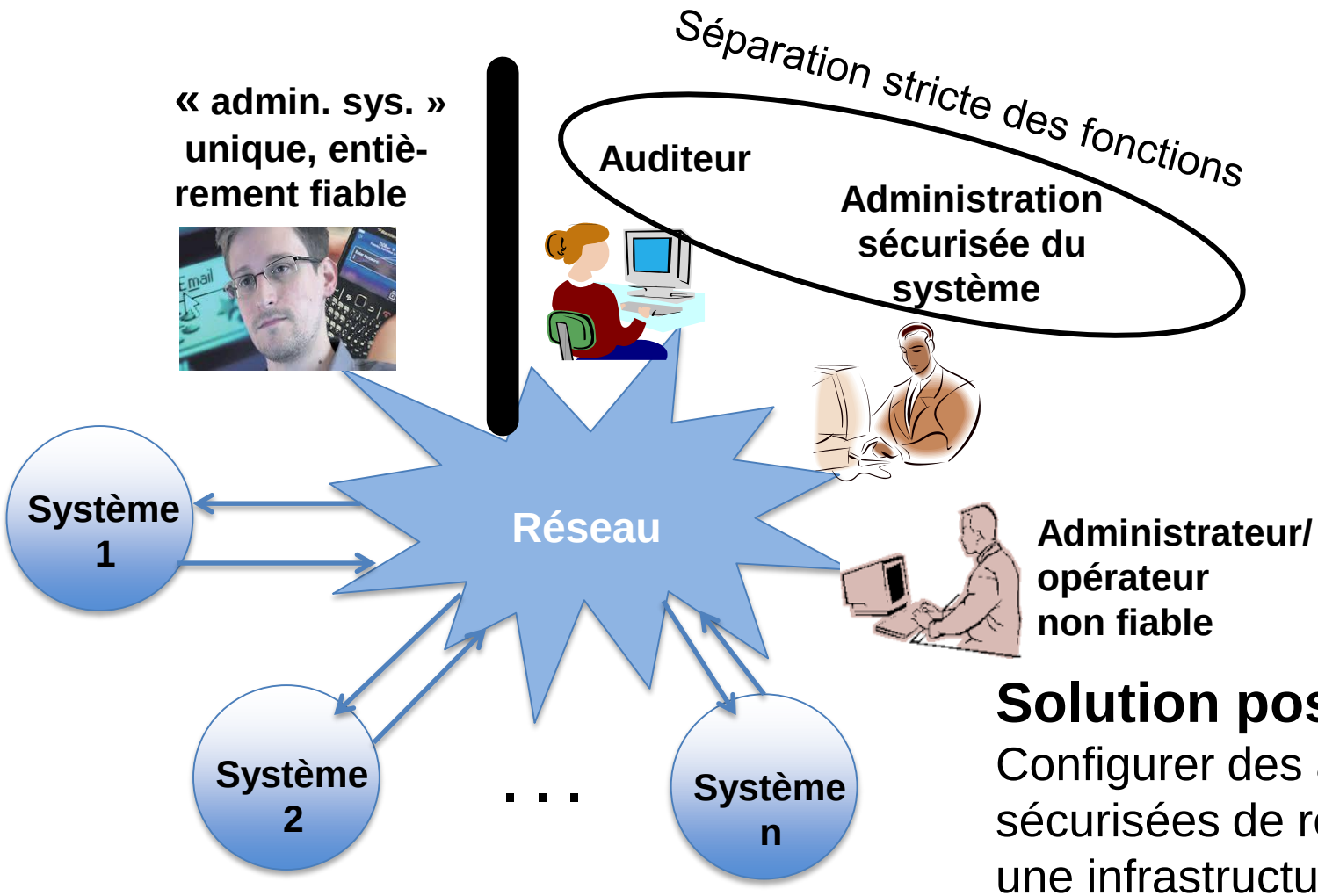
# Présence continue dans un réseau – pas un exemple de la pratique de la NSA

**- doit *rarement* établir de faux certificats**
pour des attaques HDM (intercepter les communications)
contre des protocoles chiffrés; par ex. SSL/TLS

**- doit *très rarement* utiliser des vulnérabilités «jour zéro»;**
- en 2010 utilisation de CRC-32 comme un hachage (IEEE S&P 1992)
- en 2012 attaque de collisions avec préfixes contre la fonction de hachage cryptographique MD-5 (2006-2008 TUE-EPFL)



# Administration sécurisée des réseaux: coûts (3x) et désagréments




**Solution possible:**
Configurer des administrations sécurisées de réseaux avec une infrastructure de nuages internes

# Insécurité fondamentale des systèmes/applications de commodité à code source ouvert

**Marchés des logiciels de commodité** -> **Innovation rapide** -> **Logiciels avec peu ou pas de garantie**

***Caractéristiques***
coût d'une entrée ≈ **0**
régulation ≈ **0**
responsabilité ≈ **0**

***Producteurs***
- productivité élevée; beaucoup de fonctions S/W, d'applis,
- peu de barrières pour l'utilisation d'autres codes

=> logiciels « **géants** »

***Consommateurs***
- accès à beaucoup de fonctions et applications
- prix bas

***Garantie élevée / sécurité***
- latence élevée, coût d'opportunité
- contrôle strict de la provenance
  => ne peut pas utiliser d'autres codes non vérifiés)

=> peu de fonctions; c.-à-d. **Wimps**

- coût élevé, notamment de production et de maintenance

**Marchés des logiciels de niche**

Par ex. quelques/petits segments de l'industrie aérospatiale, de défense, de l'énergie nucléaire)