Introduction à la sécurité informatique

Ayitic
Port-au-Prince, Haïti.
11 - 16 Août 2014

Lucien Loiseau

Qui suis-je ?

LUCIEN LOISEAU

- Chercheur en Informatique et télécommunication
- Thèse obtenue en 2013 à l'institut Telecom / Telecom Bretagne (Rennes, France)
- **mail :** loiseau.lucien@gmail.com

```
$ gpg --fingerprint loiseau.lucien@gmail.com
pub   2048R/F2DF8532 2012-03-21 [expire : 2017-03-20]
Empreinte de la clef = 1307 C792 1B28 28E9 554A  69E3 0916 C590 F2DF 8532
```

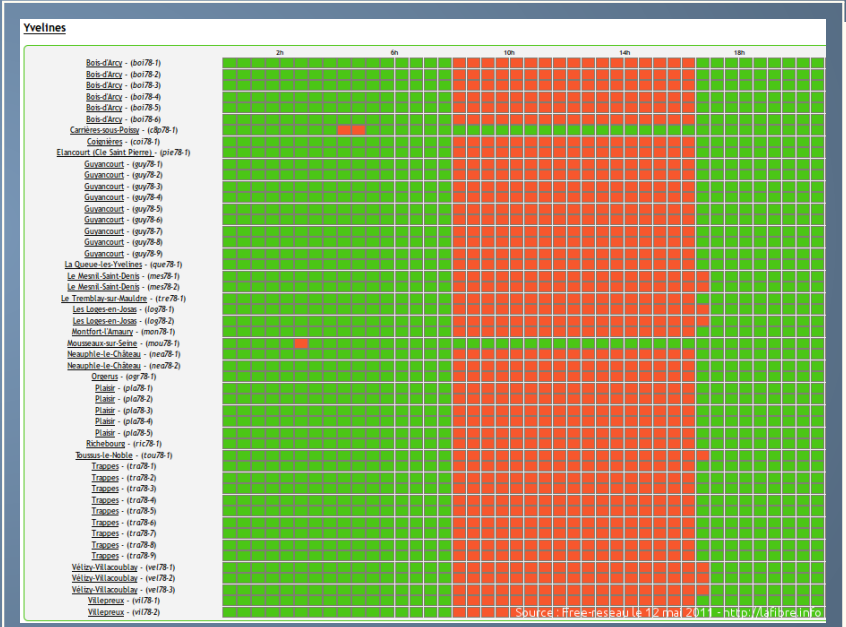
Pourquoi a-t-on besoin de la sécurité informatique ?

Les sociétés modernes sont de plus en plus dépendantes des **technologies de l'information et de la communication** (TIC)

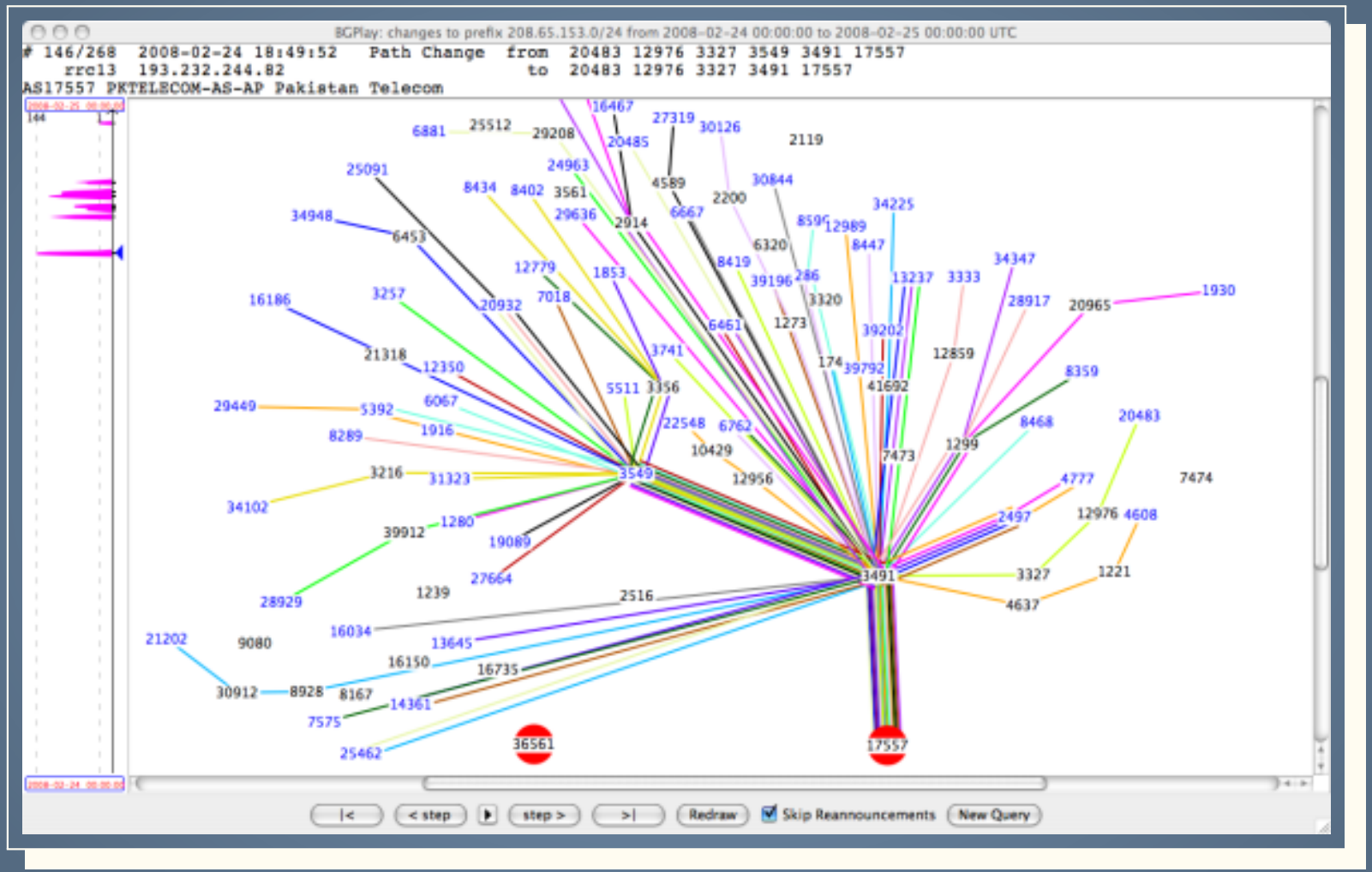
- l'informatique embarquée est en constante augmentation
- l'informatique contrôle et administre de plus en plus nos vies
- une utilisation toujours plus importantes des TICs

Coupure de fibre optique, 2011

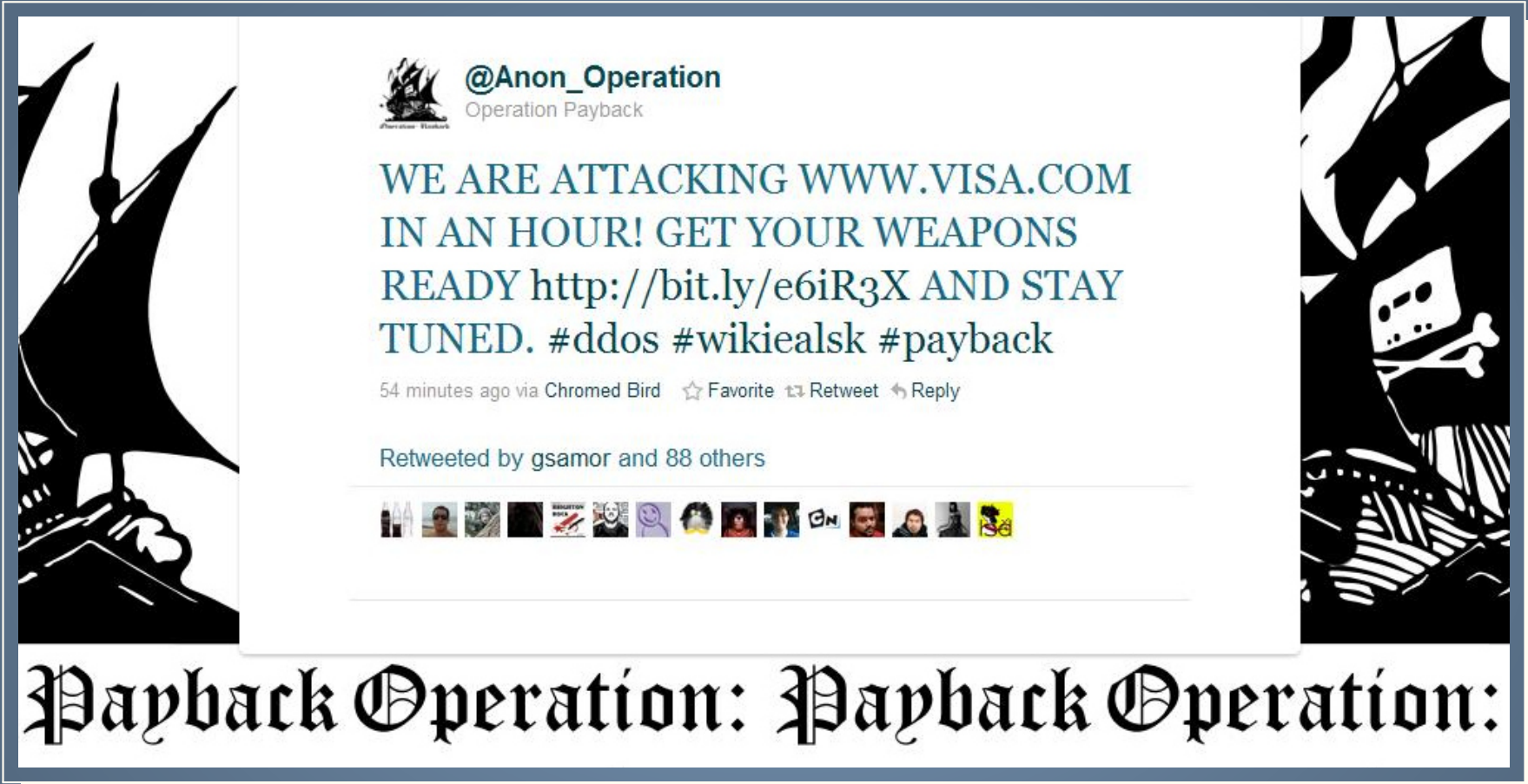
"C'est sur les travaux du Tramway reliant Vélizy à Châtillon qu'une pelleteuse à coupé plusieurs centaines de fibres au 7 avenue Morane Saulnier, à Vélizy-Villacoublay (78). Ne s'arrêtant pas en si bon chemin, la pelleteuse a également coupé des câbles EDF (sous tension) 10m plus loin. EDF étant également impacté par la coupure fibre, qui coupe son data-center."



Redirection de youtube vers le pakistan, 2008



Anonymous attaque VISA, 2012

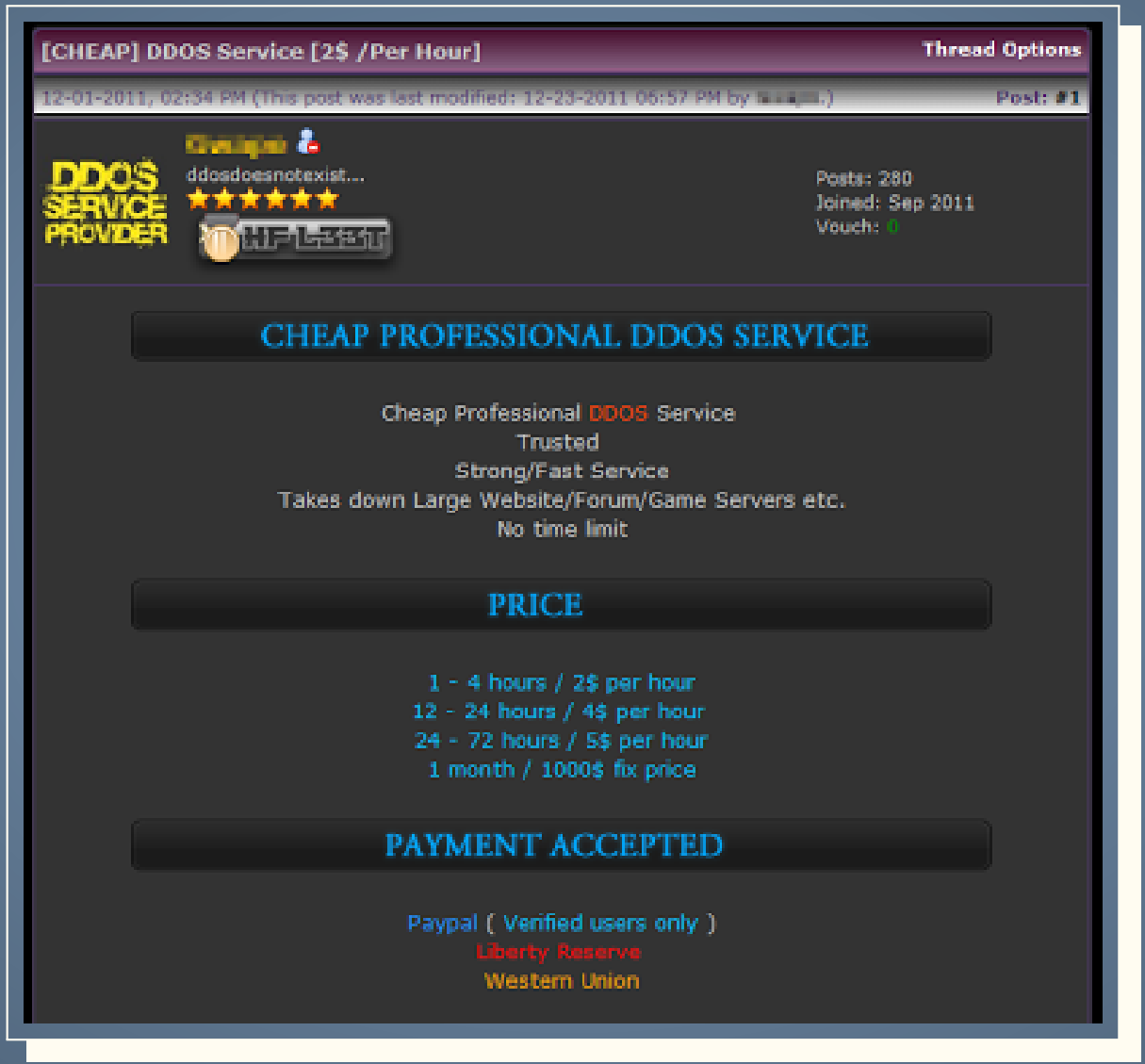


Piratage d'entreprise

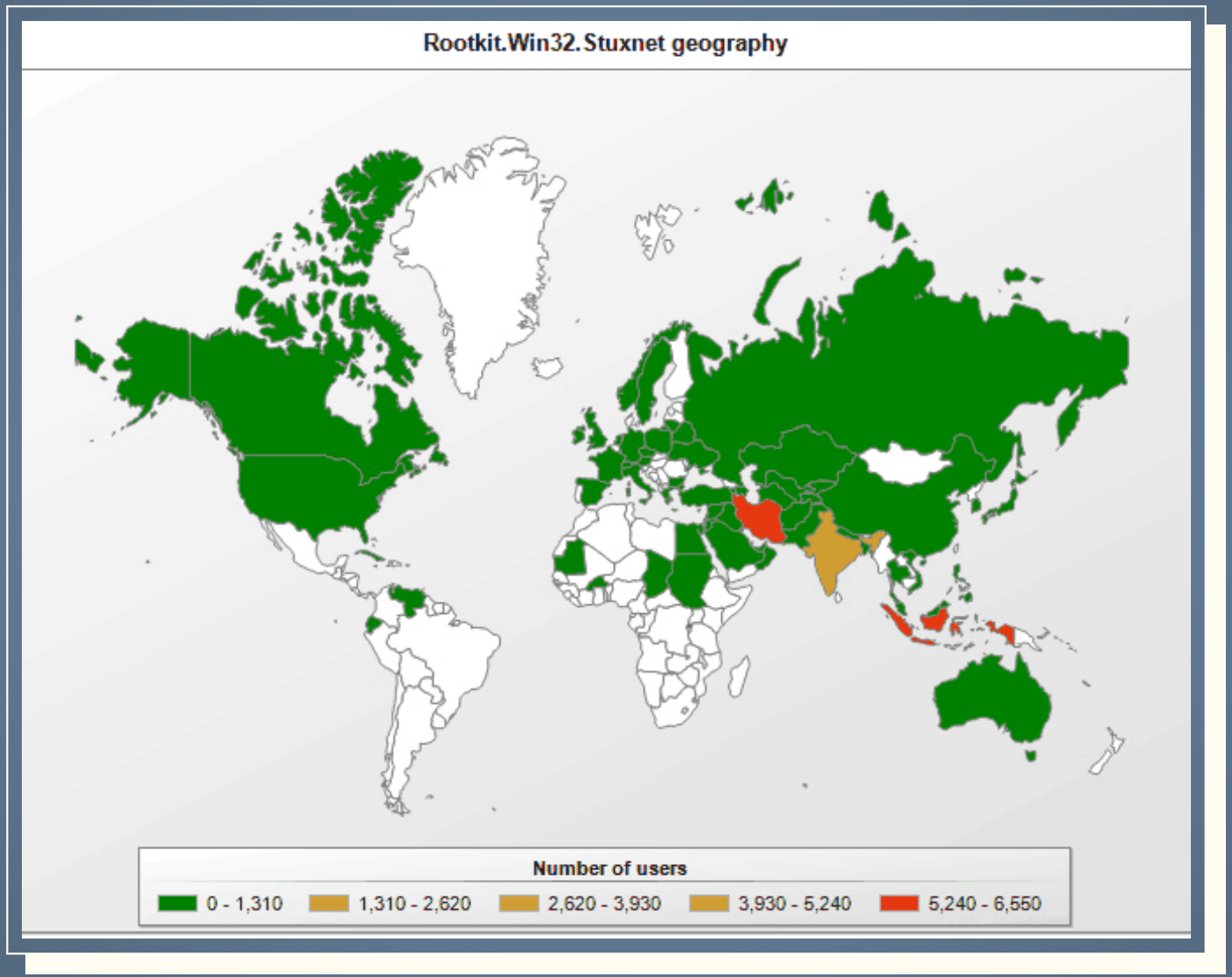
"Symantec a consulté 3 300 entreprises de trente-six pays. Intrusion dans les méandres informatiques de l'entreprise, vols de données confidentielles, usurpation d'identités d'employés, piratage et paralysie des systèmes informatiques, les opérations des pirates provoquent des dommages qui peuvent coûter cher. Ainsi, au niveau international, 20 % des entreprises évaluent les pertes annuelles causées par ces attaques à au moins 140 000 euros, imputables notamment à un ralentissement de la productivité et à la perte de données sensibles."
– *Le Monde.fr* — 07.09.2011

dernier exemple : Piratage d'Orange le 6 Mai 2014 ! (vol d'information concernant 1,3 million de personnes)

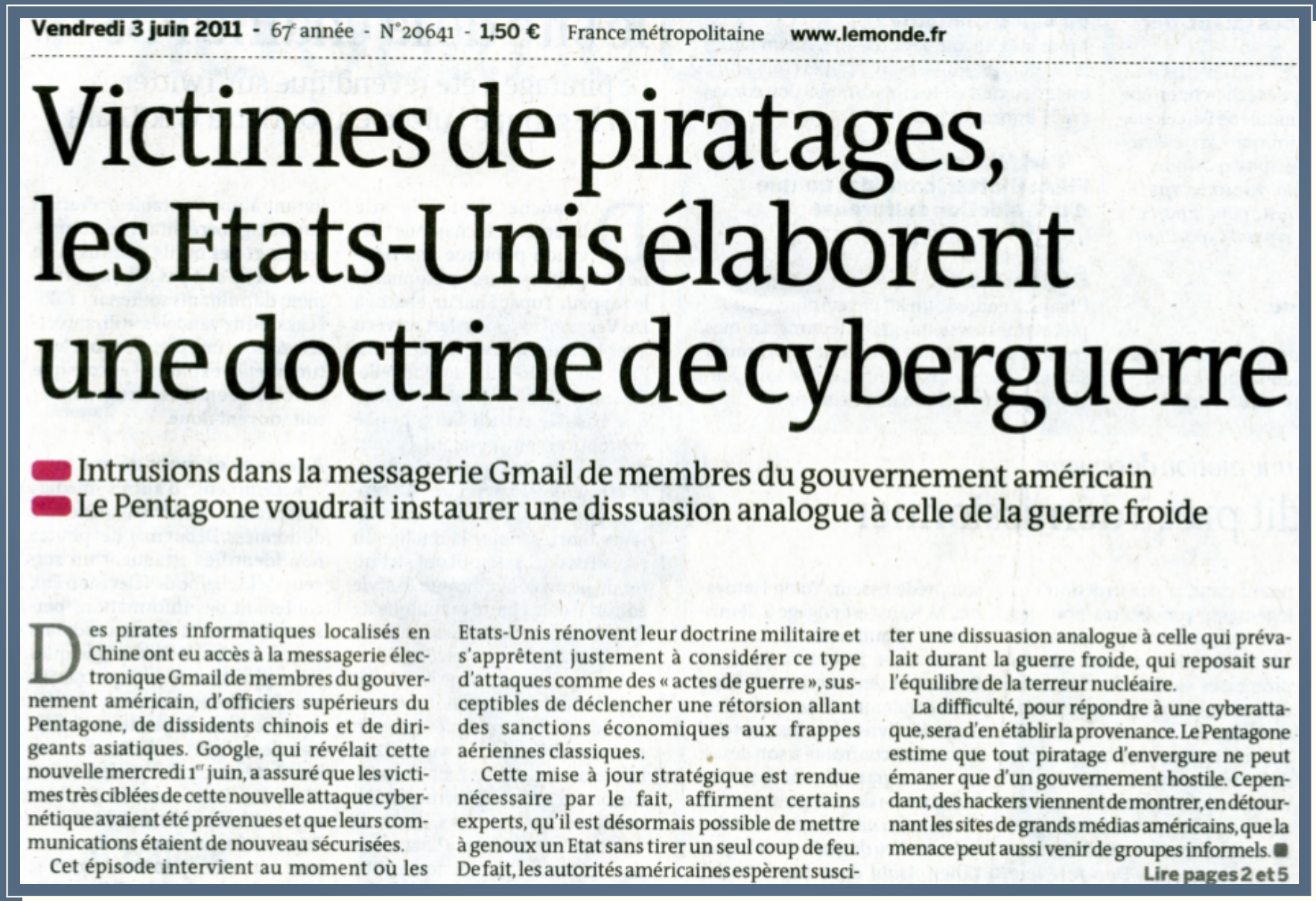
DDoS as a Service



Attaque contre l'Iran (Stuxnet) 2010



Attaque contre les États-Unis, 3 Juin 2011



Vendredi 3 juin 2011 - 67e année - N°20641 - **1,50 €** France métropolitaine **www.lemonde.fr**

Victimes de piratages, les Etats-Unis élaborent une doctrine de cyberguerre

- Intrusions dans la messagerie Gmail de membres du gouvernement américain
- Le Pentagone voudrait instaurer une dissuasion analogue à celle de la guerre froide

Des pirates informatiques localisés en Chine ont eu accès à la messagerie électronique Gmail de membres du gouvernement américain, d'officiers supérieurs du Pentagone, de dissidents chinois et de dirigeants asiatiques. Google, qui révélait cette nouvelle mercredi 1er juin, a assuré que les victimes très ciblées de cette nouvelle attaque cybernétique avaient été prévenues et que leurs communications étaient de nouveau sécurisées.

Cet épisode intervient au moment où les Etats-Unis rénovent leur doctrine militaire et s'apprêtent justement à considérer ce type d'attaques comme des « actes de guerre », susceptibles de déclencher une rétorsion allant des sanctions économiques aux frappes aériennes classiques.

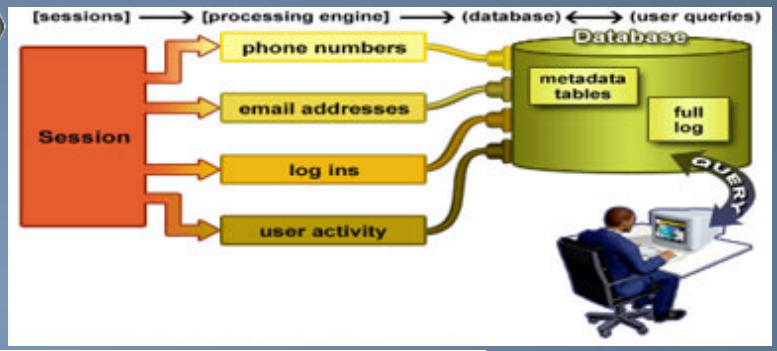
Cette mise à jour stratégique est rendue nécessaire par le fait, affirment certains experts, qu'il est désormais possible de mettre à genoux un Etat sans tirer un seul coup de feu. De fait, les autorités américaines espèrent susciter une dissuasion analogue à celle qui prévalait durant la guerre froide, qui reposait sur l'équilibre de la terreur nucléaire.

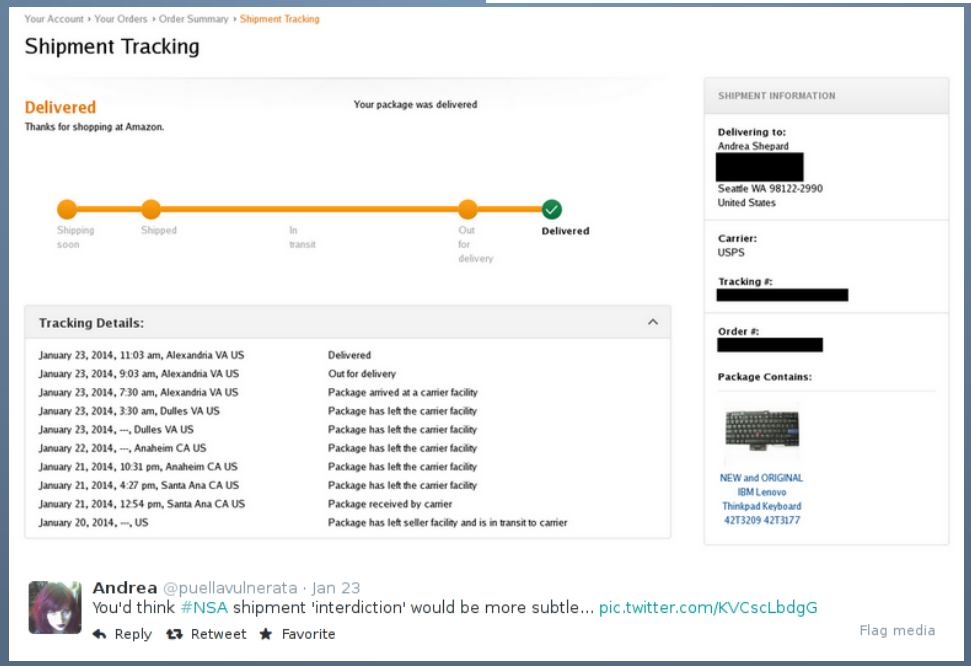
La difficulté, pour répondre à une cyberattaque, sera d'en établir la provenance. Le Pentagone estime que tout piratage d'envergure ne peut émaner que d'un gouvernement hostile. Cependant, des hackers viennent de montrer, en détournant les sites de grands médias américains, que la menace peut aussi venir de groupes informels. ■

Lire pages 2 et 5

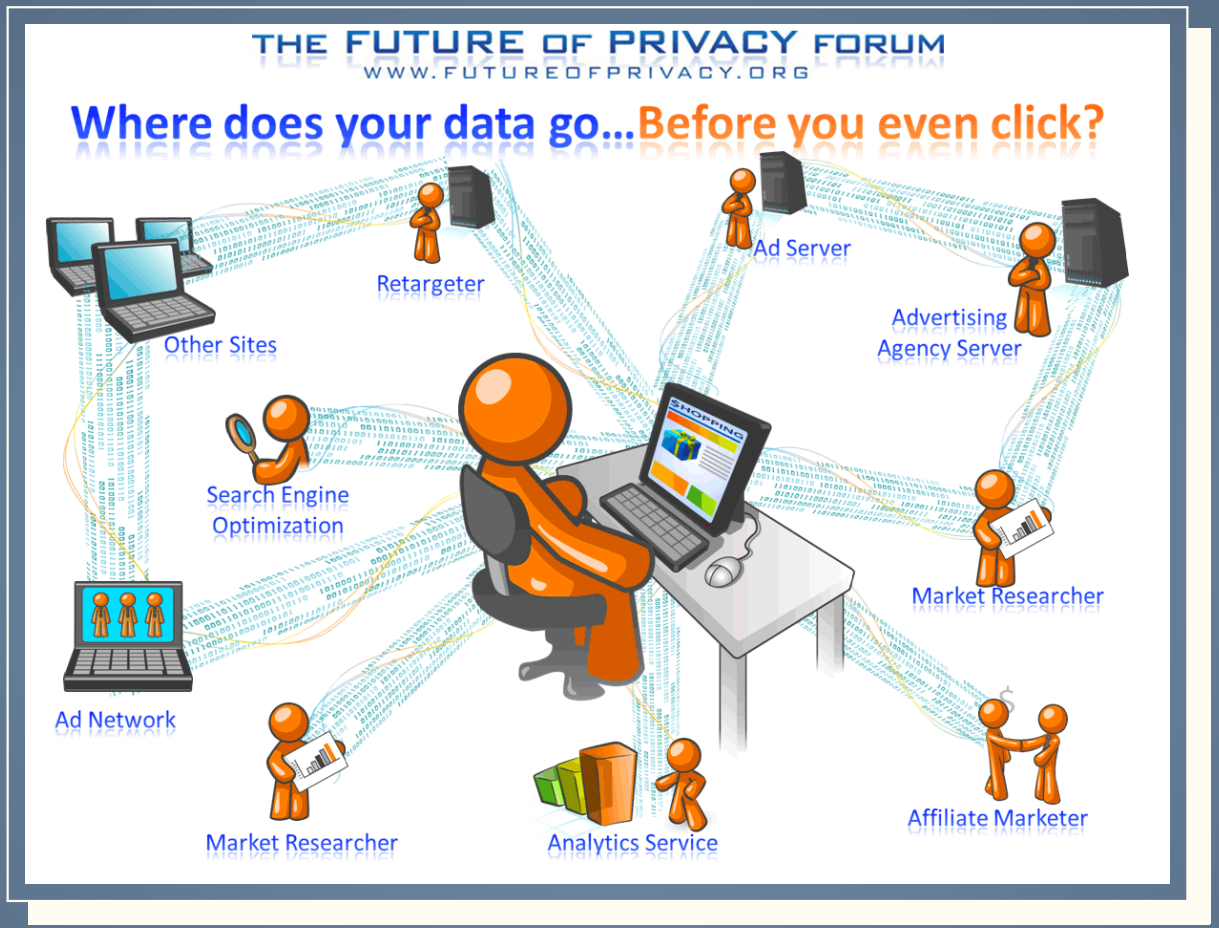
L'affaire Snowden, 2013 (1/2)

L'affaire Snowden, 2013 (2/2)



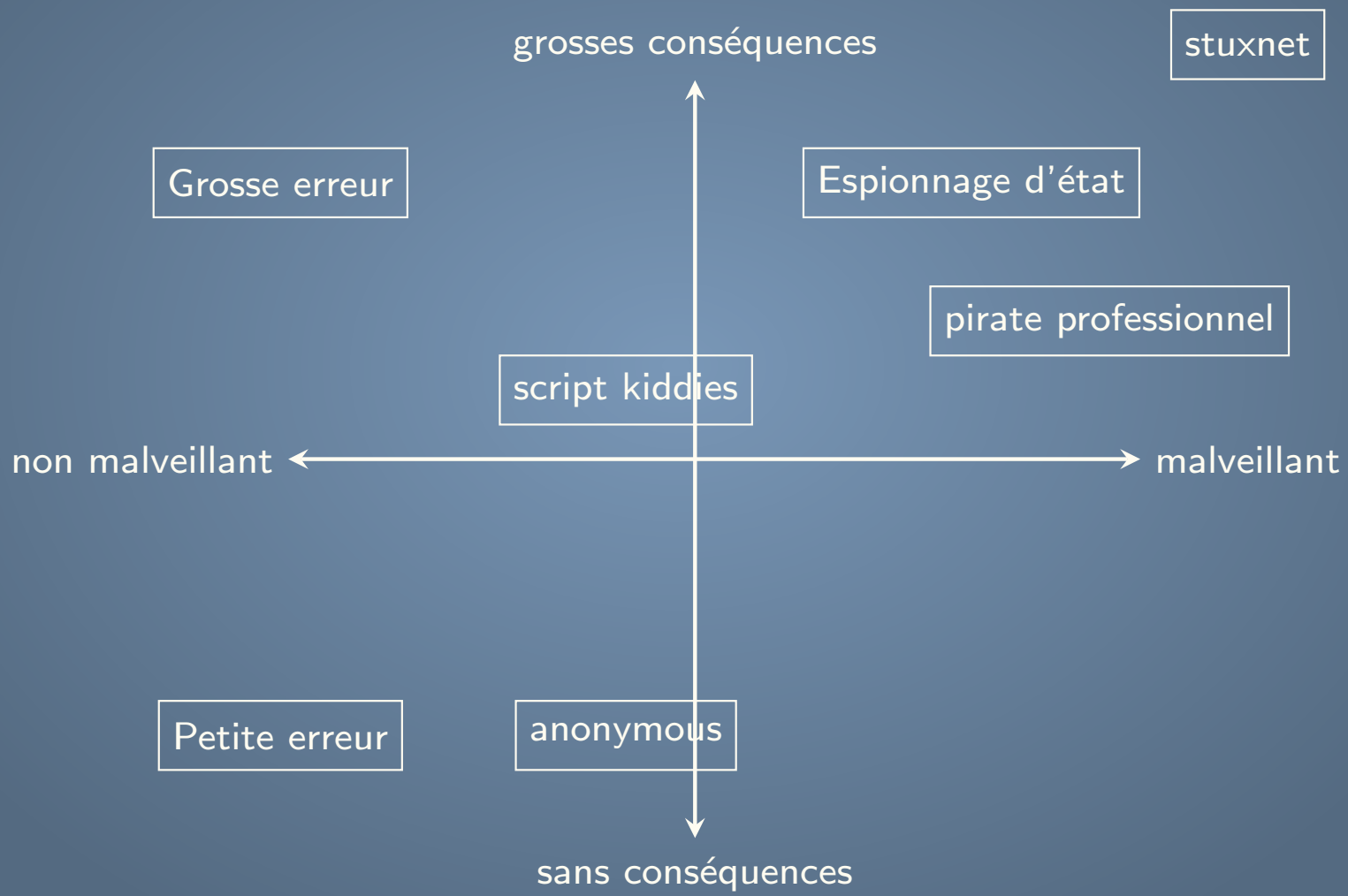


La vie privée mise à mal par les états mais aussi par les entreprises



La liberté d'expression victime elle aussi d'attaques informatique

Des attaquants divers aux motivations variées



Un vaste domaine

La sécurité informatique concerne tout le monde :

- **Les individus** : vie privée de l'individu, journaliste, ONG etc.
- **Les entreprises** : protection des systèmes d'information, des infrastructures etc.
- **Les états** : cyberguerre (cyberpaix ?), espionnage etc.

La sécurité informatique s'attache à sécuriser :

- **Le matériel** : puces, téléphones, fermes de serveurs, etc.
- **Le software** : système d'exploitation, programmes, site web, etc.
- **Les données** : fichiers, bases de données, etc.
- **Les canaux de communications** : wifi, GSM, Bluetooth, téléphone portables

Le paradigme Vulnérabilité - Menace - Contrôle

Un des buts de la sécurité c'est de protéger des ressources

- **Vulnérabilité** : une faiblesse dans le système.
- **Menaces** : Si il y a une vulnérabilité, une situation nuisible peu survenir
- **Contrôle** : Permet de réduire l'effet d'une vulnérabilité

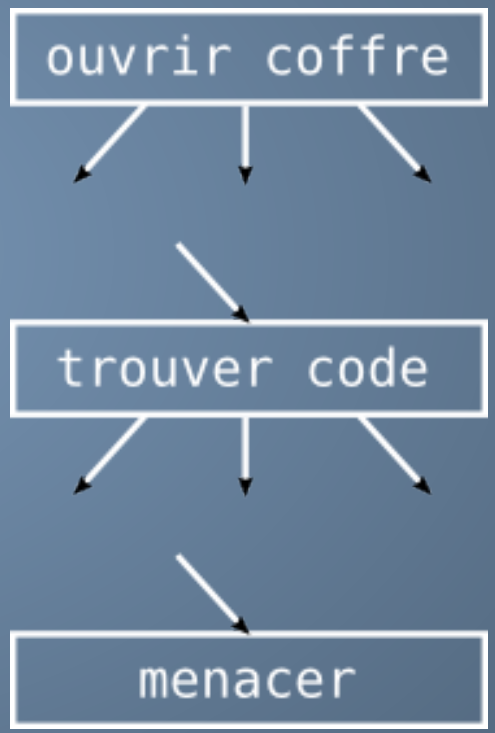
→ Les **menaces** sont bloqués en **contrôlant** les **vulnérabilités** !

Modéliser les menaces : Les arbres d'attaques

But d'un attaquant : Ouvrir le coffre

Modéliser les menaces : Les arbres d'attaques

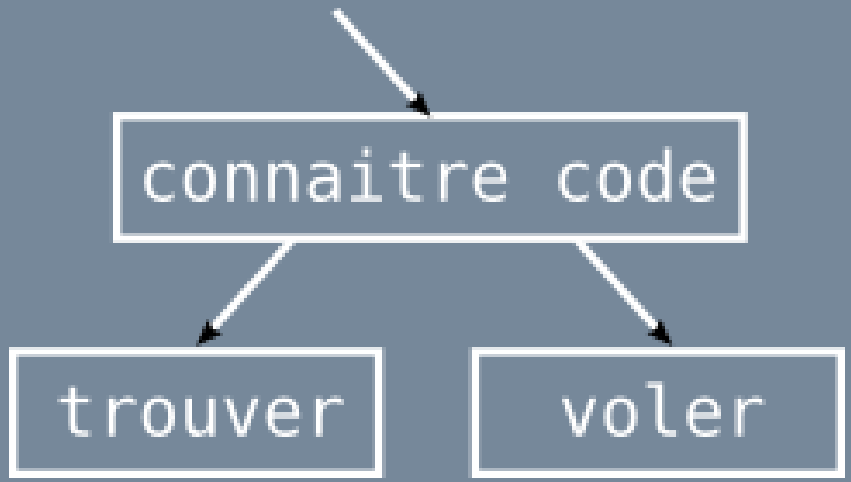
- **Le But** : ce que veut l'attaquant
- **Les Étapes** : décomposition du but
- **Les Feuilles** : Actions



Modéliser les menaces : Les arbres d'attaques

La disjonction

- C'est le OU logique

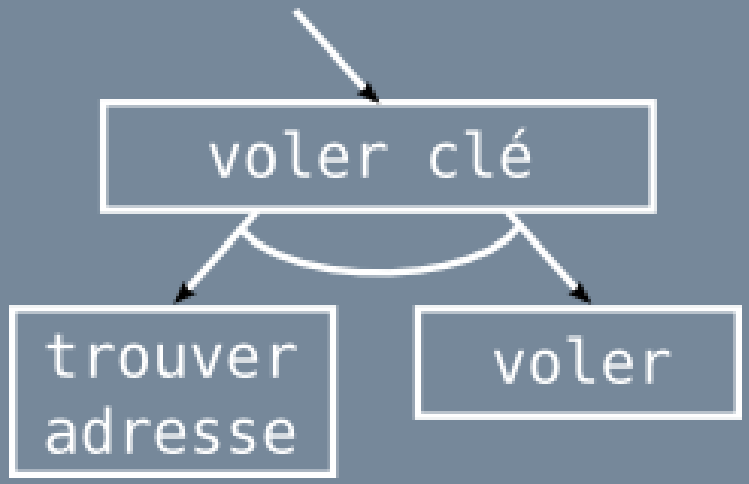


- Une étape est obtenue en satisfaisant **au moins une** des sous étapes

Modéliser les menaces : Les arbres d'attaques

La conjonction

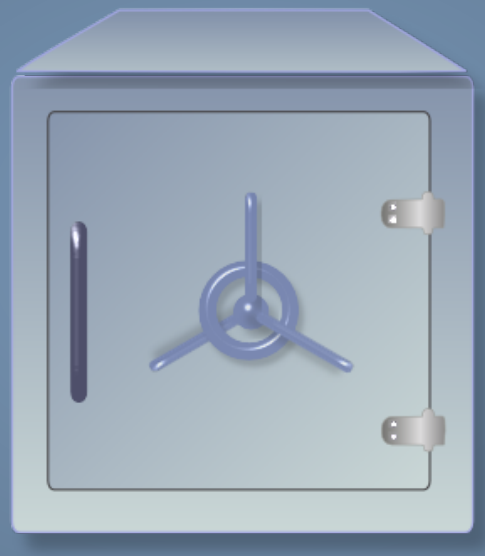
- C'est le ET logique



- Une étape est obtenue en satisfaisant **toutes** les sous étapes

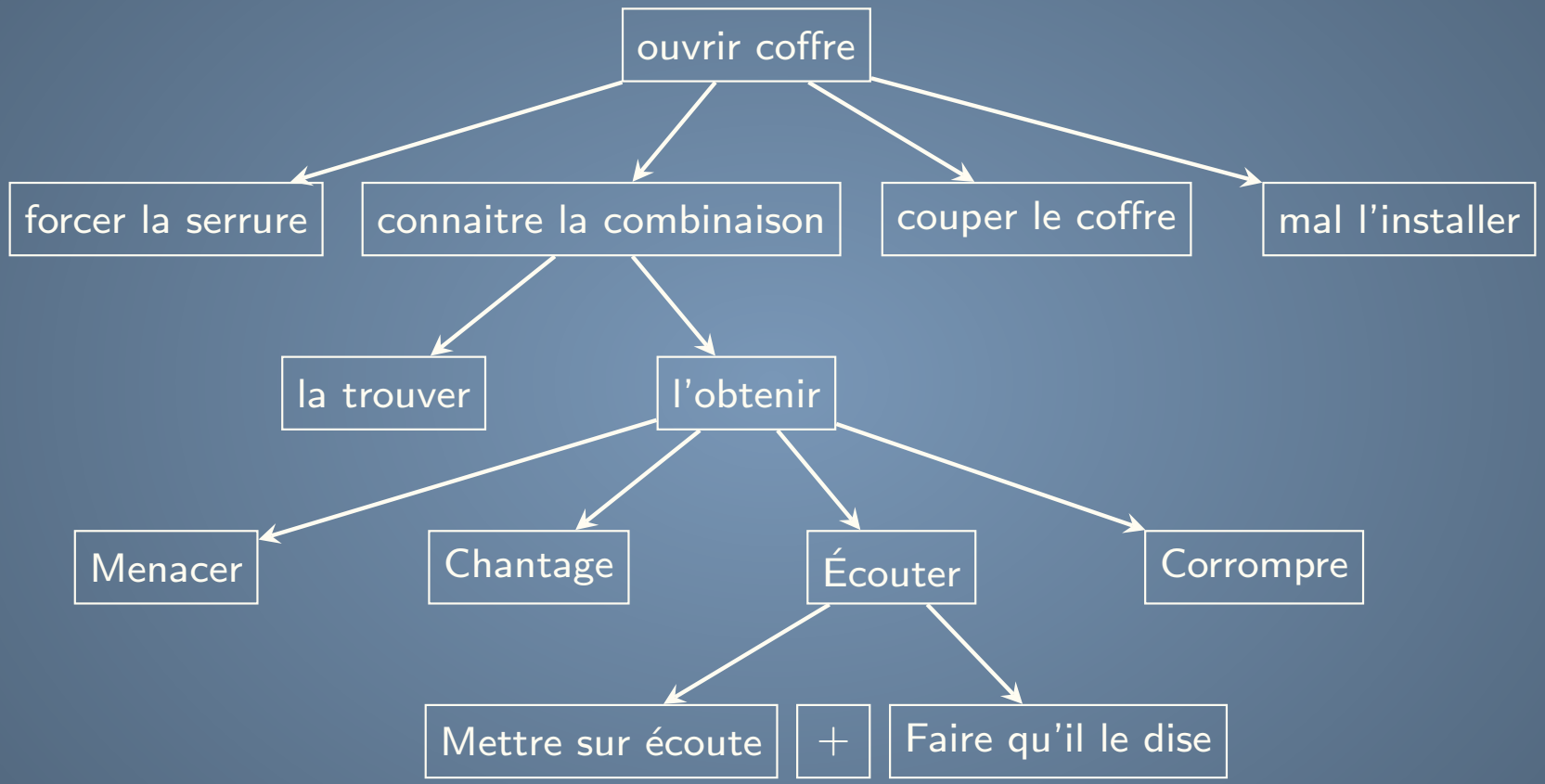
Modéliser les menaces : Les arbres d'attaques

But d'un attaquant : Ouvrir le coffre



Exercice : Modélisez la menace avec un arbre d'attaque

Modéliser les menaces : Les arbres d'attaques

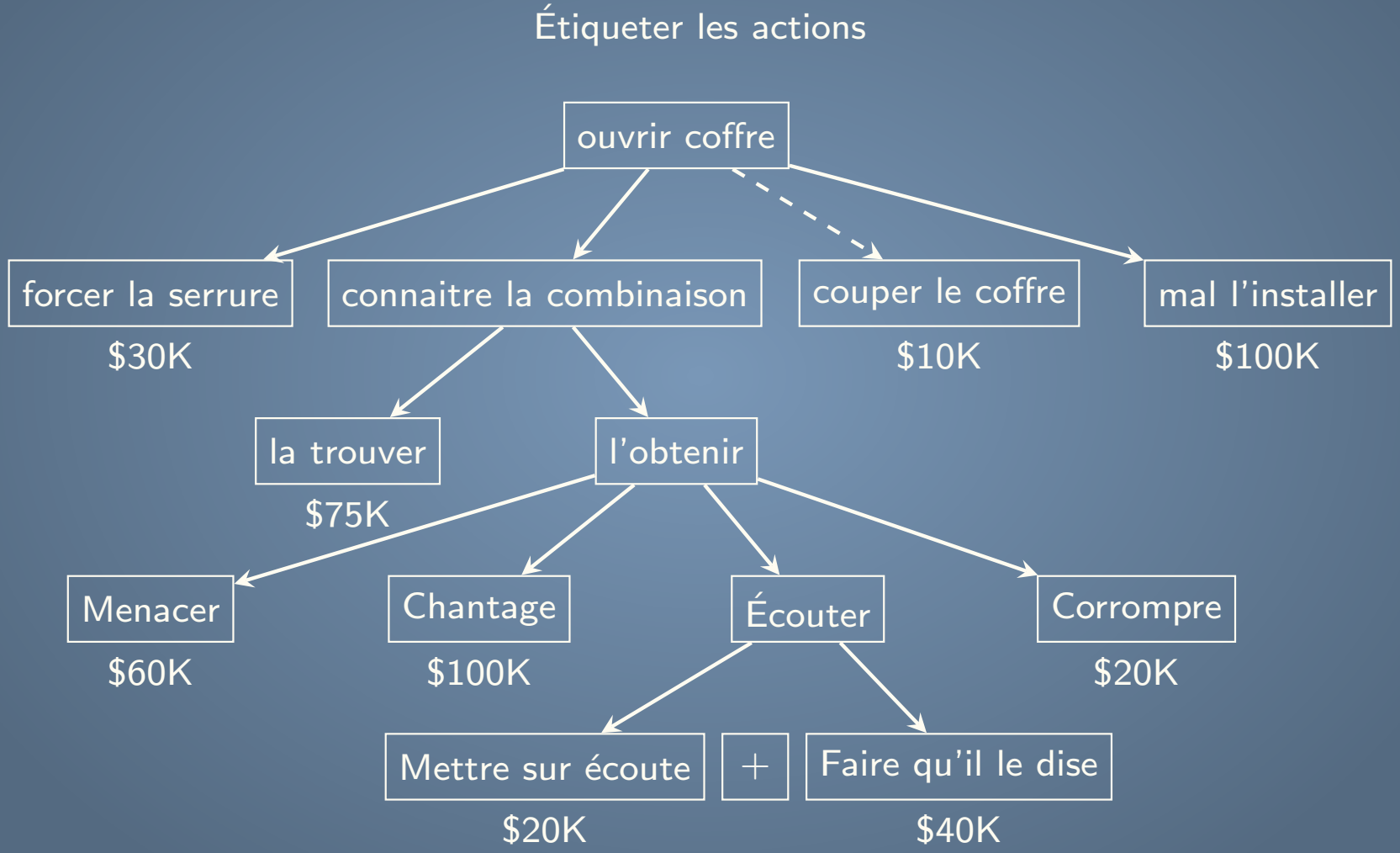


Modéliser les menaces : Les arbres d'attaques

Les feuilles peuvent être étiquettées

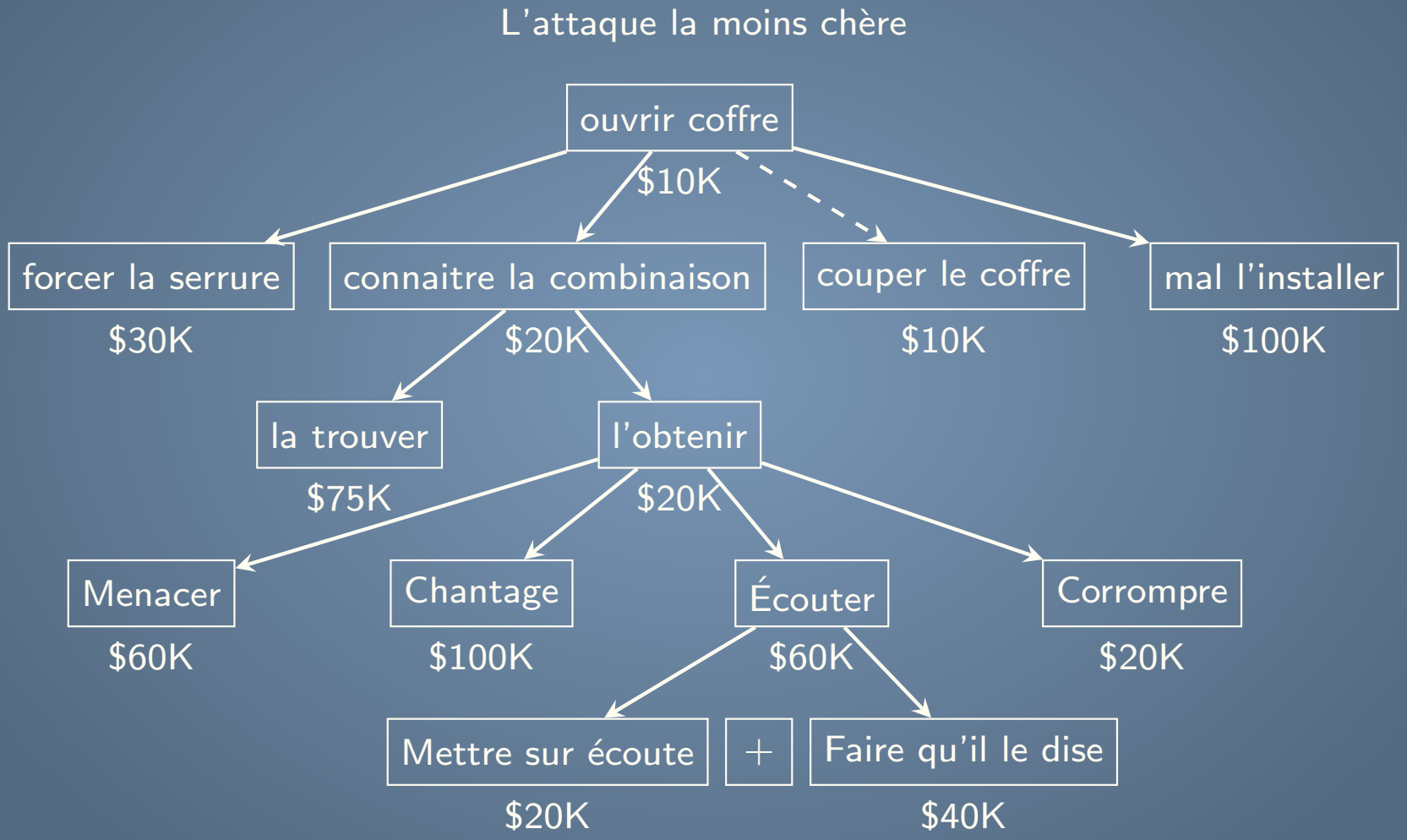
- Possible/Impossible
- Coût de l'action : 10 euros...
- Durée de l'action : 3 min, 1 jour...
- Le multi-étiquetage est possible

Modéliser les menaces : Les arbres d'attaques



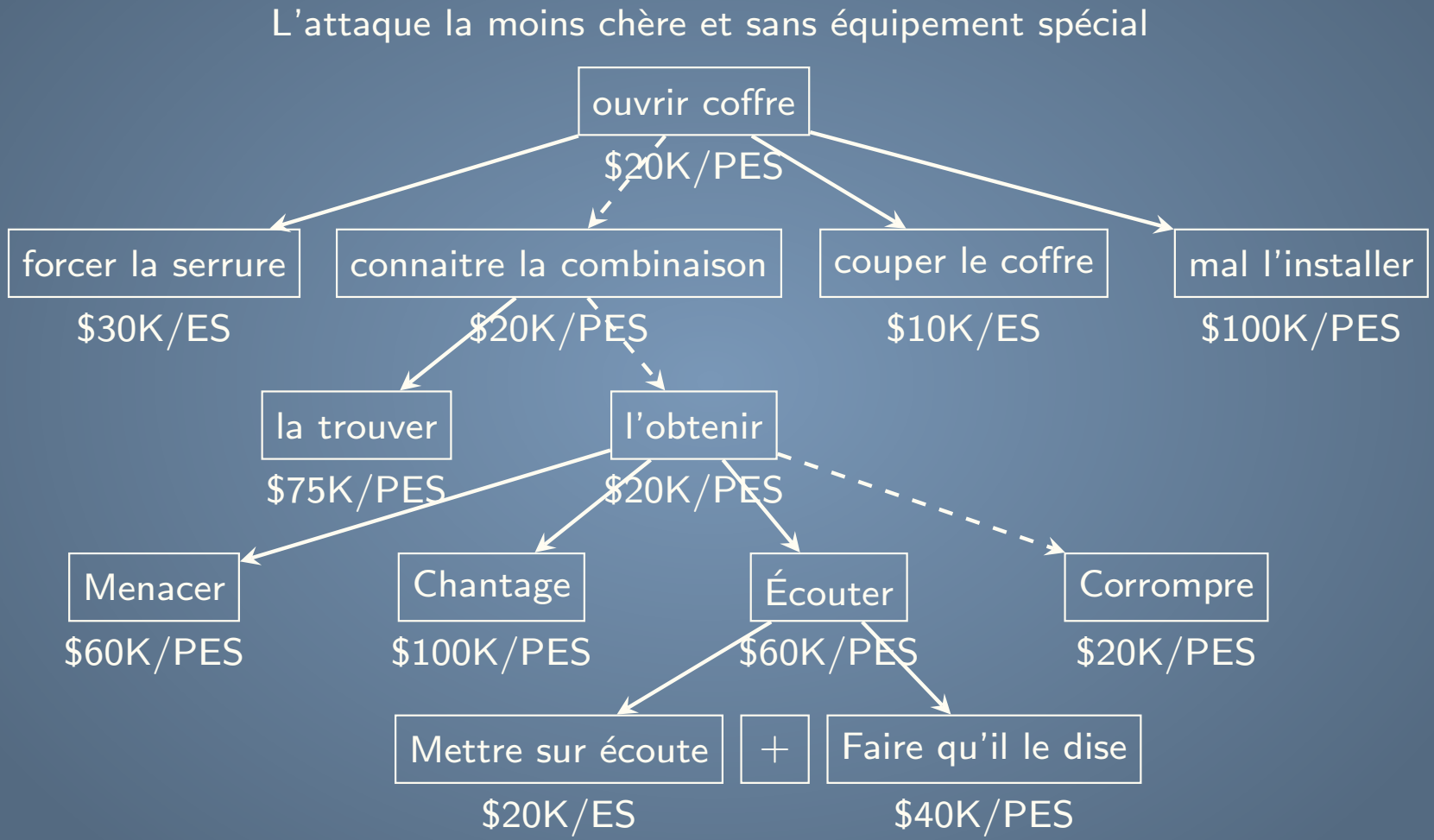
$ = cout de l'attaque

Modéliser les menaces : Les arbres d'attaques



$ = cout de l'attaque

Modéliser les menaces : Les arbres d'attaques



$ = cout de l'attaque
ES = Équipement Special
PES = Pas d'Équipement Special

Modéliser les menaces : Les arbres d'attaques

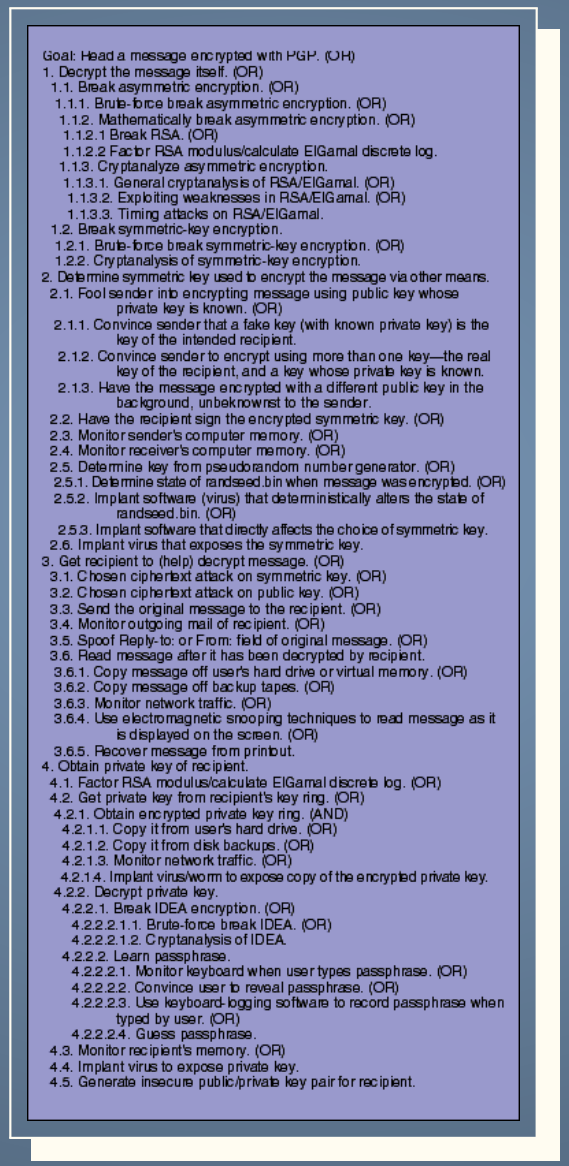
Avantages

Incrémentalité :	facile à faire évoluer
Requêtes :	trouver les attaques possible selon différents critères
Comparaison :	comparer des systèmes

Inconvénients

Construction :	Exhaustivité *vs* synthèse
Lisibilité :	Illisible au delà de 20 nœuds, perte d'intuition
Théorique :	Manque d'expressivité ("sauf si", "à moins que", "ou exclusif", etc.)

Modéliser les menaces : Les arbres d'attaques



Goal: Read a message encrypted with PGP. (OR)
1. Decrypt the message itself. (OR)
 1.1. Break asymmetric encryption. (OR)
  1.1.1. Brute-force break asymmetric encryption. (OR)
  1.1.2. Mathematically break asymmetric encryption. (OR)
   1.1.2.1 Break RSA. (OR)
   1.1.2.2 Factor RSA modulus/calculate ElGamal discrete log.
  1.1.3. Cryptanalyze asymmetric encryption.
   1.1.3.1. General cryptanalysis of RSA/ElGamal. (OR)
   1.1.3.2. Exploiting weaknesses in RSA/ElGamal. (OR)
   1.1.3.3. Timing attacks on RSA/ElGamal.
 1.2. Break symmetric-key encryption.
  1.2.1. Brute-force break symmetric-key encryption. (OR)
  1.2.2. Cryptanalysis of symmetric-key encryption.
2. Determine symmetric key used to encrypt the message via other means.
 2.1. Fool sender into encrypting message using public key whose private key is known. (OR)
  2.1.1. Convince sender that a fake key (with known private key) is the key of the intended recipient.
  2.1.2. Convince sender to encrypt using more than one key—the real key of the recipient, and a key whose private key is known.
  2.1.3. Have the message encrypted with a different public key in the background, unbeknownst to the sender.
 2.2. Have the recipient sign the encrypted symmetric key. (OR)
 2.3. Monitor sender's computer memory. (OR)
 2.4. Monitor receiver's computer memory. (OR)
 2.5. Determine key from pseudorandom number generator. (OR)
  2.5.1. Determine state of randseed.bin when message was encrypted. (OR)
  2.5.2. Implant software (virus) that deterministically alters the state of randseed.bin. (OR)
  2.5.3. Implant software that directly affects the choice of symmetric key.
 2.6. Implant virus that exposes the symmetric key.
3. Get recipient to (help) decrypt message. (OR)
 3.1. Chosen ciphertext attack on symmetric key. (OR)
 3.2. Chosen ciphertext attack on public key. (OR)
 3.3. Send the original message to the recipient. (OR)
 3.4. Monitor outgoing mail of recipient. (OR)
 3.5. Spoof Reply-to: or From: field of original message. (OR)
 3.6. Read message after it has been decrypted by recipient.
  3.6.1. Copy message off user's hard drive or virtual memory. (OR)
  3.6.2. Copy message off backup tapes. (OR)
  3.6.3. Monitor network traffic. (OR)
  3.6.4. Use electromagnetic snooping techniques to read message as it is displayed on the screen. (OR)
  3.6.5. Recover message from printout.
4. Obtain private key of recipient.
 4.1. Factor RSA modulus/calculate ElGamal discrete log. (OR)
 4.2. Get private key from recipient's key ring. (OR)
  4.2.1. Obtain encrypted private key ring. (AND)
   4.2.1.1. Copy it from user's hard drive. (OR)
   4.2.1.2. Copy it from disk backups. (OR)
   4.2.1.3. Monitor network traffic. (OR)
   4.2.1.4. Implant virus/worm to expose copy of the encrypted private key.
  4.2.2. Decrypt private key.
   4.2.2.1. Break IDEA encryption. (OR)
    4.2.2.1.1. Brute-force break IDEA. (OR)
    4.2.2.1.2. Cryptanalysis of IDEA.
   4.2.2.2. Learn passphrase.
    4.2.2.2.1. Monitor keyboard when user types passphrase. (OR)
    4.2.2.2.2. Convince user to reveal passphrase. (OR)
    4.2.2.2.3. Use keyboard-logging software to record passphrase when typed by user. (OR)
    4.2.2.2.4. Guess passphrase.
 4.3. Monitor recipient's memory. (OR)
 4.4. Implant virus to expose private key.
 4.5. Generate insecure public/private key pair for recipient.

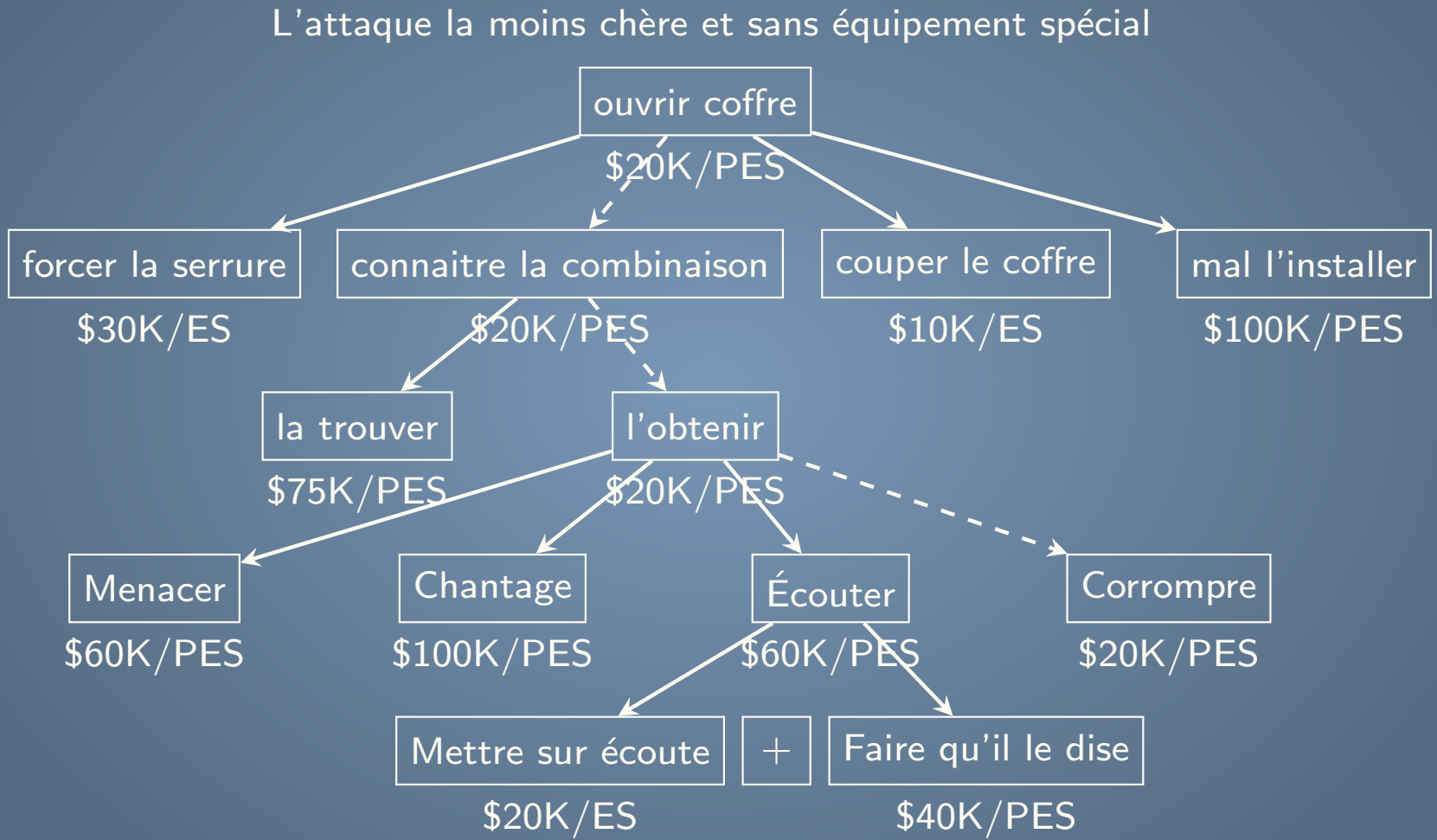
FIGURE: Arbre d'attaque (version texte) de l'application GnuPG

Méthodes de défense

Les 6 approches pour défendre un système d'information

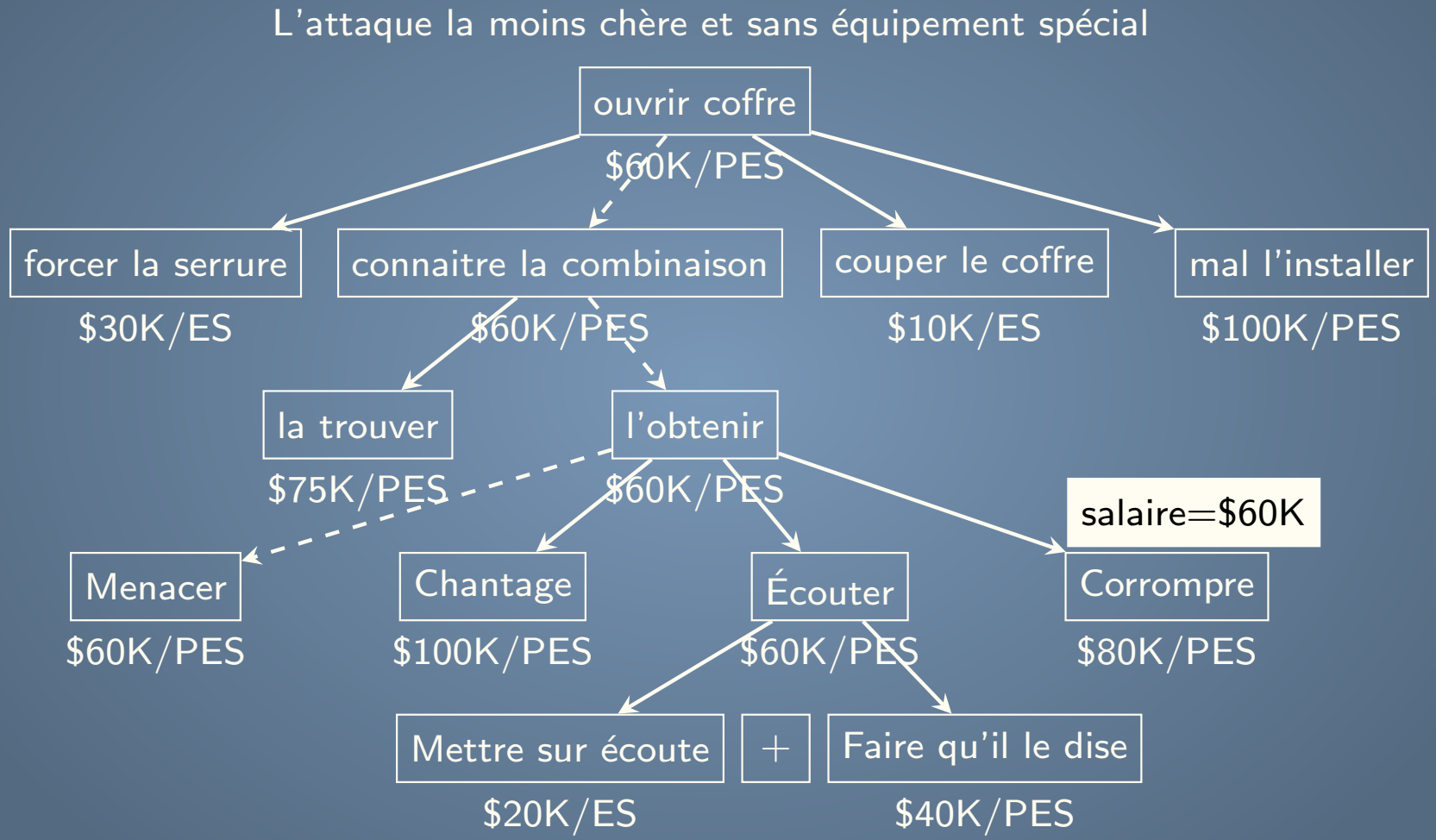
1. Empêcher l'attaque
   - Bloquer l'attaque / Clore la vulnérabilité (e.g. réparer les bugs d'un code)
2. Prévenir l'attaque
   - Rendre l'attaque plus difficile (e.g. chiffrement)
3. Dévier l'attaque
   - Rendre une autre cible plus attractive (e.g. honeypot)
4. Atténuer l'attaque
   - Rendre l'impact d'une attaque moins sévère (e.g. cloisonner les services)
5. Détecter une attaque
   - Pendant ou après (e.g. alarme de voiture)
6. Se remettre d'une attaque (e.g. backup)

Modéliser les menaces : Les arbres d'attaques



$ = cout de l'attaque
ES = Équipement Special
PES = Pas d'Équipement Special

Modéliser les menaces : Les arbres d'attaques



$ = cout de l'attaque
ES = Équipement Special
PES = Pas d'Équipement Special

Organisation du workshop

- **Lundi** (aujourd'hui) : Sécurité de l'information (Partie 2)
  - → mettre la cryptographie dans son contexte historique
  - → Les algorithmes de chiffrement symétriques
- **Mardi** : Sécurité de l'information (Partie 2)
  - → Les algorithmes de chiffrement asymétriques
  - → Intégrité, Signature
- **Mercredi** : Sécurité offensives des réseaux
  - → Scanner un réseau
  - → Attaque MITM
- **Jeudi** : Sécurité défensive des réseaux - SSL
  - → Comprendre le 'S' de HTTPS
- **Vendredi** : Wargame