Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 26 nov. 2009

"Appréhender les menaces
quand les risques sont exacerbés en période de crise"

Puis, la crise avait fini par les atteindre directement. L'un perdit son emploi ...
un autre claquait des dents et touchait du bois (Marcel AYME, Maison basse, p. 169).

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 26 nov. 2009

"Appréhender les menaces
quand les risques sont exacerbés en période de crise"

Les cybermenaces et l'IE

La place des entreprises et de la gendarmerie nationale

Les territoires du Rhin supérieur

par le Général d'armée
Marc WATIN-AUGOUARD

Inspecteur général des armées - gendarmerie

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 26 nov. 2009

"Appréhender les menaces
quand les risques sont exacerbés en période de crise"

Puis, la crise avait fini par les atteindre directement. L'un perdit son emploi ...
un autre claquait des dents et touchait du bois (Marcel AYME, Maison basse, p. 169).

Forum du Rhin supérieur sur les Cybermenaces

Salle des conférences de l'ENA à Strasbourg le 26 nov. 2009

"Appréhender les menaces
quand les risques sont exacerbés en période de crise"

Evolution des cybermenaces et période de crise

Email : guinier@acm.org

par Daniel GUINIER

Expert judiciaire près la Cour d'Appel de Colmar
Dr ès Sciences, Certifications CISSP, ISSMP, ISSAP, MBCI
Lieutenant-colonel (RC) de la gendarmerie nationale

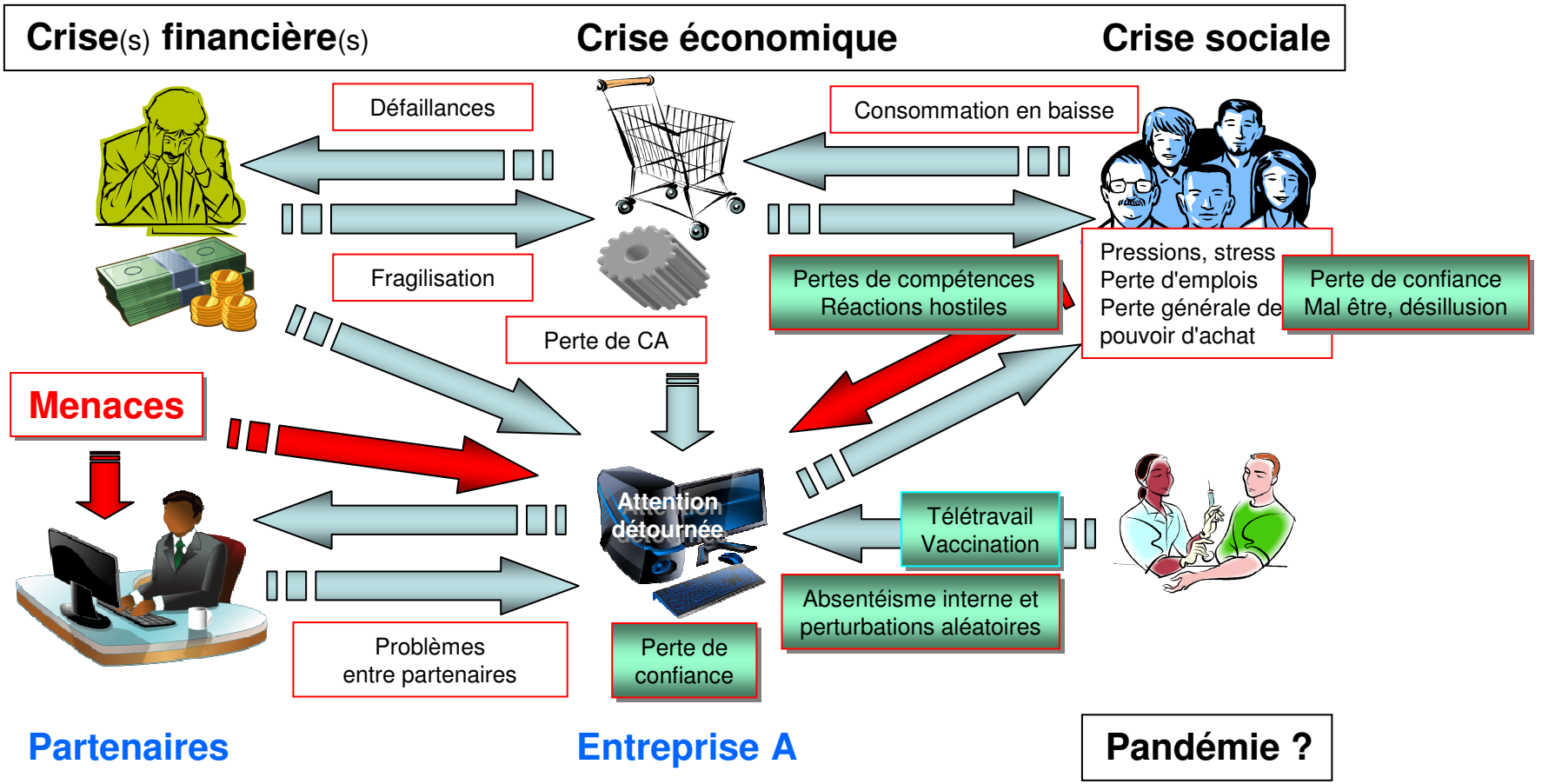
Eléments communs relevant des crises

Caractéristiques des crises

- **Une perte de repères** liée à son caractère brutal
- **Une crise naît** souvent :
  - de défaillances multiples et quasi-simultanées
  - de phénomènes qui se produisent en cascade
  - de liens entre les systèmes connectés
- **Une crise révèle** souvent :
  - des scénarios jugés improbables ou imprévisibles
  - des conditions préalables sous-estimées ou ignorées
  - des déficits chroniques vis-à-vis du danger

Une menace sérieuse de cyber-pandémie est une situation de crise, et pas un simple dysfonctionnement.

Existence de crises conjuguées



Si les conditions initiales forment les conditions du chaos, les crises multiples favorisent la recherche du profit : fraude, détournement de données, concurrence déloyale, etc.

Les cybermenaces et leur évolution

Problématique

- **Interconnexion** des systèmes
- **Fragmentation** et **perméabilité** des systèmes
- **Dépendance** forte au SI *(pour 75 % des entreprises (Clusif (2006)))*
- **Monoculture** et peu de **diversité technologique**
- **Sous-estimation** du risque : *complexité, externalisation, etc.*

- **La cible** est l'information et sa valeur stratégique
- **La cybercriminalité** est organisée et industrialisée
- **La crise** exacerbe les menaces :
  - plus d'actes criminels motivés
  - moins de moyens pour la sécurité

Les PME-PMI sont plutôt isolées et peu sensibilisées tandis que la criminalité est organisée et essentiellement motivée par le profit, ce qui nécessite une stratégie de défense.

Cybermenaces et risque - Définitions

- **Cybermenace** - *Menace liée aux TIC*
  - Action visant l'information ou le système d'information (SI)
  - Conséquences possibles sur l'organisme entier
- **Vulnérabilité**
  - Point de faiblesse de la sécurité, faille
  - Contexte *(ex. déficit de sécurité, période de crise)*
- **Cible**
  - Sensibilité - *liée à la confidentialité*
  - Vitalité - *liée à la disponibilité*
  - Valeur - *liée au coût de remplacement*
- **Risque**
  - Caractérisation du risque : *[Menace – Vulnérabilité – Cible]*
  - Exposition au risque : *[Possibilité de réalisation – Impact]*

La cybercriminalité concerne les infractions pénales commises à l'encontre des TIC et de l'information, mais aussi à l'aide des TIC pour commettre, favoriser ou masquer des délits et crimes.

Enoncé des cybermenaces

Sensible & Vital
Sensible
Vital
Image

Vol de composants, de systèmes, de périphériques : PDA, portables, et de supports : disques, clés USB, etc.

Dans 90 % des cas la perte totale des données conduit à la fermeture de l'entreprise.

Interception de données, "reniflage", perçage de mots de passe, décryptage, capture des rayonnements EM, WiFi, etc.

Enlèvement
C, D, T

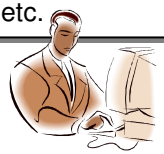
Sabotage physique, incendie, destruction des sauvegardes, ou tous autres dégâts volontaires.

Interception
C

Destruction
D, T

Corruption, manipulation, ingénierie sociale, *"stagiaire" / "candidat"* cheval de Troie, intoxication chimique ou virale, atteinte physique, etc.

Information négative, désinformation, diffamation publique, mise en cause dans procès en cours, condamnation pénale ou civile, etc.



Dégradation d'image

Divulgation
C

Interruption
D, T

Divulgation de données sensibles, personnelles ou classifiées, de savoir-faire, vol de données, espionnage.

Déni de service (DoS) ou déni de service distribué (D-DoS)

Modification
I, T

Perturbation
D, T

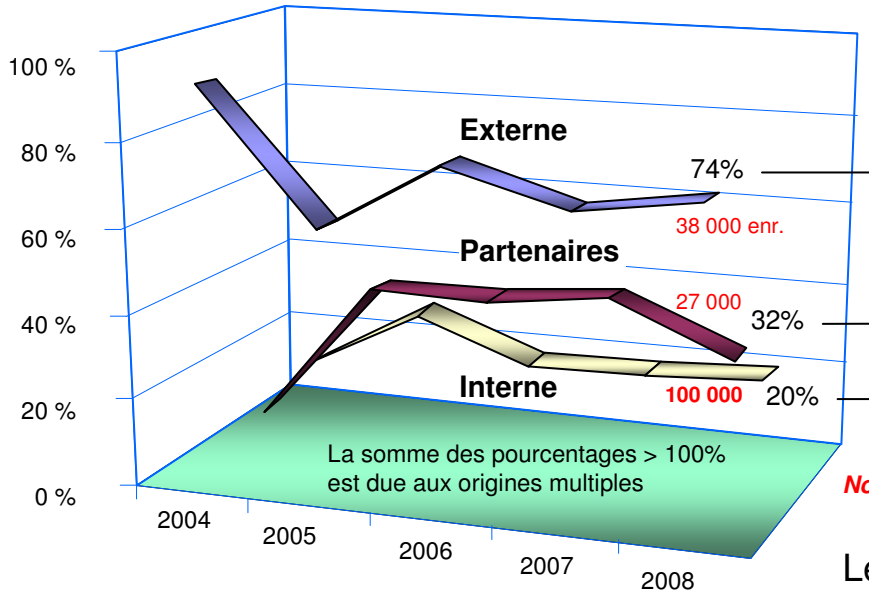
Piratage, code malveillant, mystification d'adresse, modification de données, fraude, défiguration de site, etc.

Réduction de l'efficacité par des attaques logiques ou physiques, ou émissions parasitaires, détournement d'activité.

La compromission d'un attribut de la sécurité : Confidentialité (C), Intégrité (I), Disponibilité (D) , peut en affecter un autre, ainsi que l'impuTabilité (T), du fait d'interdépendances.

Sources d'incidents

Source : Verizonbusiness (2009) : 2009 Data Breach Investigations Report



Globalement sur 5 années

Année 2008

43 % uniquement externe ;
exposition au risque : 28

39 % sources multiples

7 % uniquement du fait de partenaires ;
exposition au risque : 9

11 % uniquement interne ;
exposition au risque : 20

Nombre moyen d'enregistrements compromis par incident

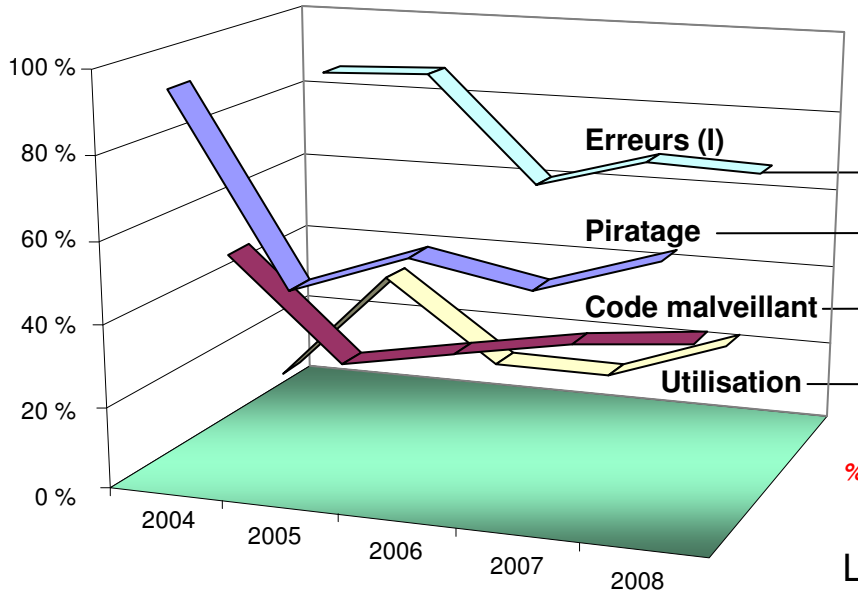
Les incidents de source interne continuent cependant à provoquer individuellement plus de dommages.

Dans la plupart des cas, les incidents sont facilités par un relâchement dans les bonnes pratiques de sécurité, ce qui nécessite aussi plus de visibilité et de contrôle entre partenaires.

Le pourcentage d'incidents lié aux partenaires a quintuplé du fait de l'externalisation et du partage entre partenaires.

Catégories d'incidents

Source : Verizonbusiness (2009) : 2009 Data Breach Investigations Report



Année 2008

67 % indirectement liés à des erreurs

64 % liés au piratage *(**94 %** enr.)*

38 % liés à des virus, chevaux de Troie, etc, *(**90 %** enr.)*

30 % liés directement à une utilisation impropre

% de compromissions parmi 285 millions d'enregistrements

Globalement sur 5 années

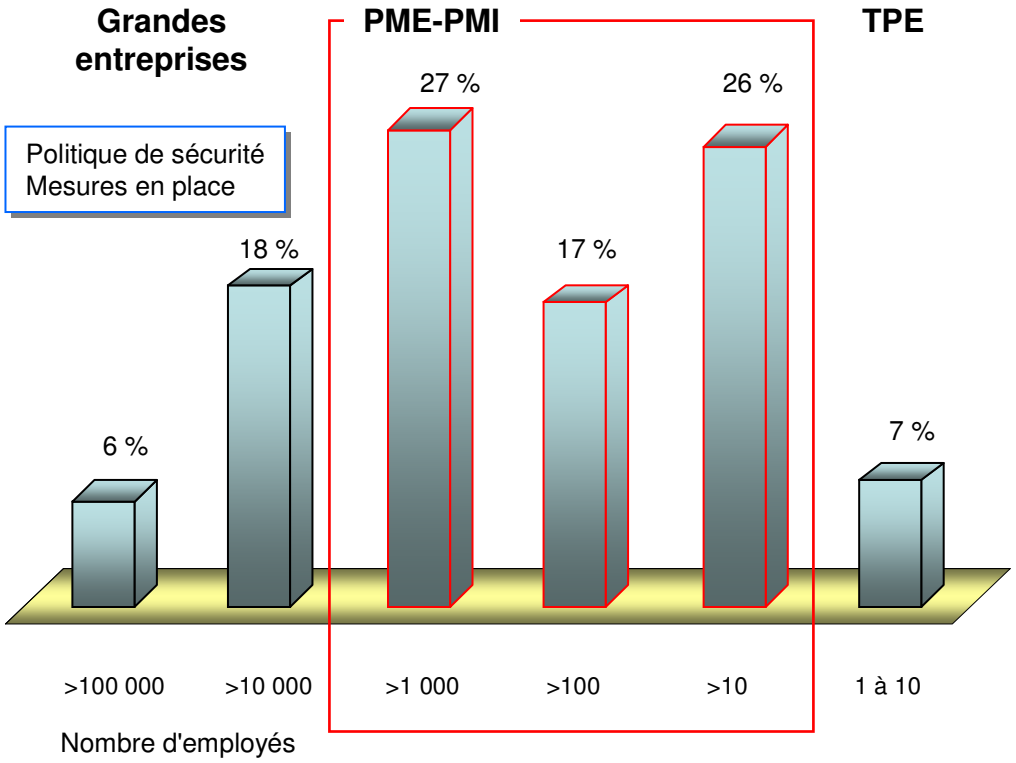
Les incidents indirectement liés aux erreurs (I) sont importants (67 %), comparés à ceux qui sont directement liés aux erreurs (1 %).

Infections par un code malveillant : installé majoritairement par l'attaquant : 18 %, contre 7% du fait de navigation Web
Ces codes malveillants proviennent à 59 % de développements, contre 21 % à 29 % avant cela de 2004 à 2007.

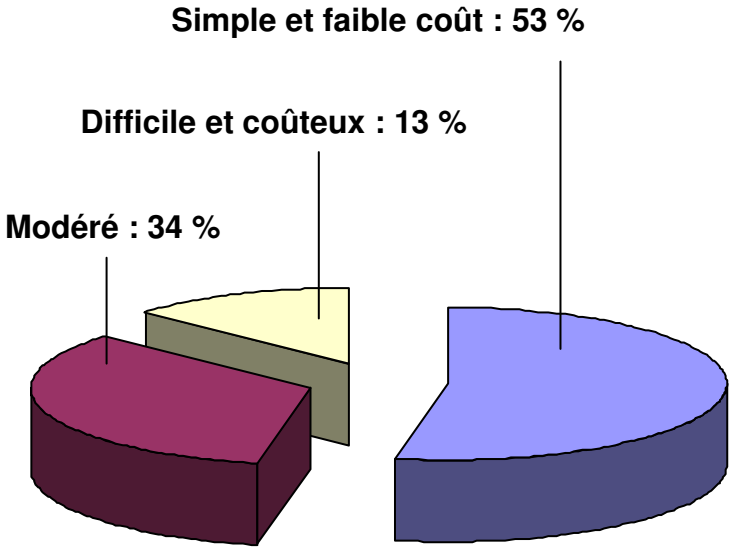
D'où le scénario-type : l'attaquant prend avantage des fautes pour commettre un piratage à distance, installer un code malveillant, et collecter des informations confidentielles.

Victimes d'incidents et mesures

Source : Verizonbusiness (2009) : 2009 Data Breach Investigations Report



Victimes en % d'incidents



Effort et dépenses nécessaires pour les mesures d'évitement des incidents

Les PME sont les plus atteintes, tandis que l'effort et les dépenses nécessaires aux contre-mesures de sécurité sont en majorité simples et peu coûteuses dans l'ensemble.

Ex. Attaques par Bluetooth réalisables

Bluetooth est une alternative aux communications infrarouge (IrDA) fondée sur une technologie radio ondes courtes. Elle permet la transmission des données au travers d'obstacles hors vue à la fréquence de l'ordre de 2,4 GHz tout comme la technologie WiFi 802.11 ; le spectre de fréquence utilisé varie en fonction de la réglementation des pays.

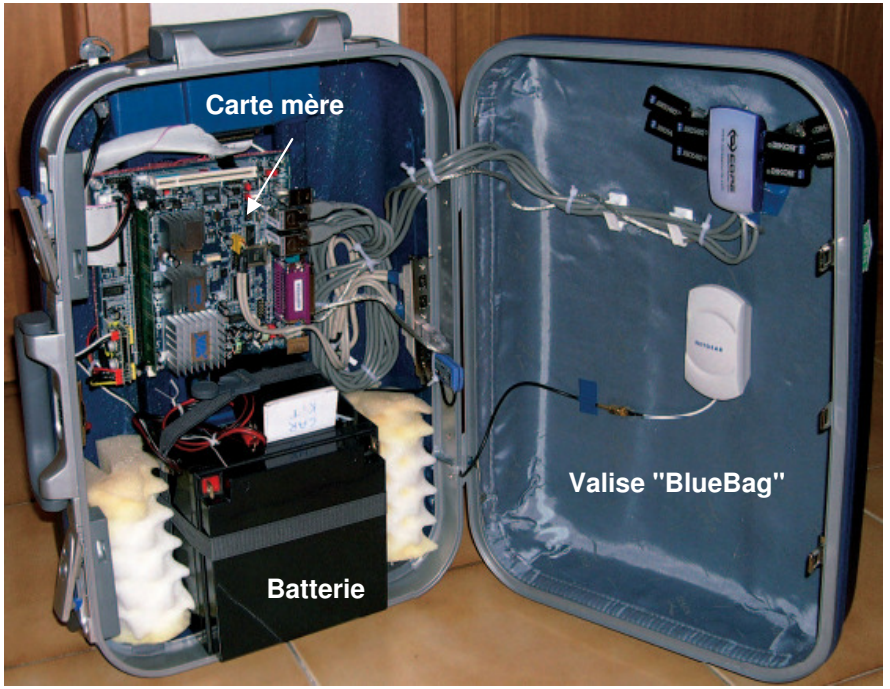
- 12 500 unités Bluetooth actives détectées à 100 mètres, en une semaine l'exposition CeBIT 2006 à Hanovre.

Répartition des unités actives Bluetooth	%
Téléphones mobiles	93,4%
PC portables	2,8%
PDA	1,5%
GPS	1,1%
Imprimantes	0,4%
Autres	0,9%

Convergence

Projet *"**BlueBag**"* montrant la faisabilité d'attaques ciblées au travers d'une connexion Bluetooth, au moyen de codes malveillants, et par le fait que 7,5% des personnes sont potentiellement victimes d'ingénierie sociale en acceptant le téléchargement de fichiers de sources inconnues.

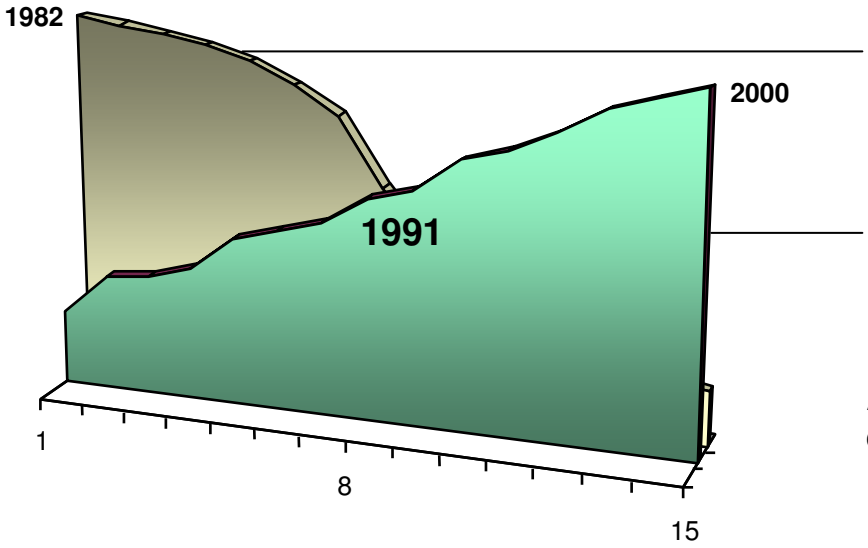
Les simulations indiquent **un taux de contamination jusqu'à 98 % en moins de 10 mn**, dans le cas d'un *"ver"* **pour ces 7,5 % - *soit près de 920 unités contaminées !***



Voir Carettoni L. et al. (2007), *IEEE Security & Privacy, mars-avril, pp.17-25)*

Constats similaires à divers salons, expositions, aéroports, universités, etc., avec un taux de détection de 1 à 5 par mn.

De la "piraterie" ...



Niveau d'expertise général des attaquants

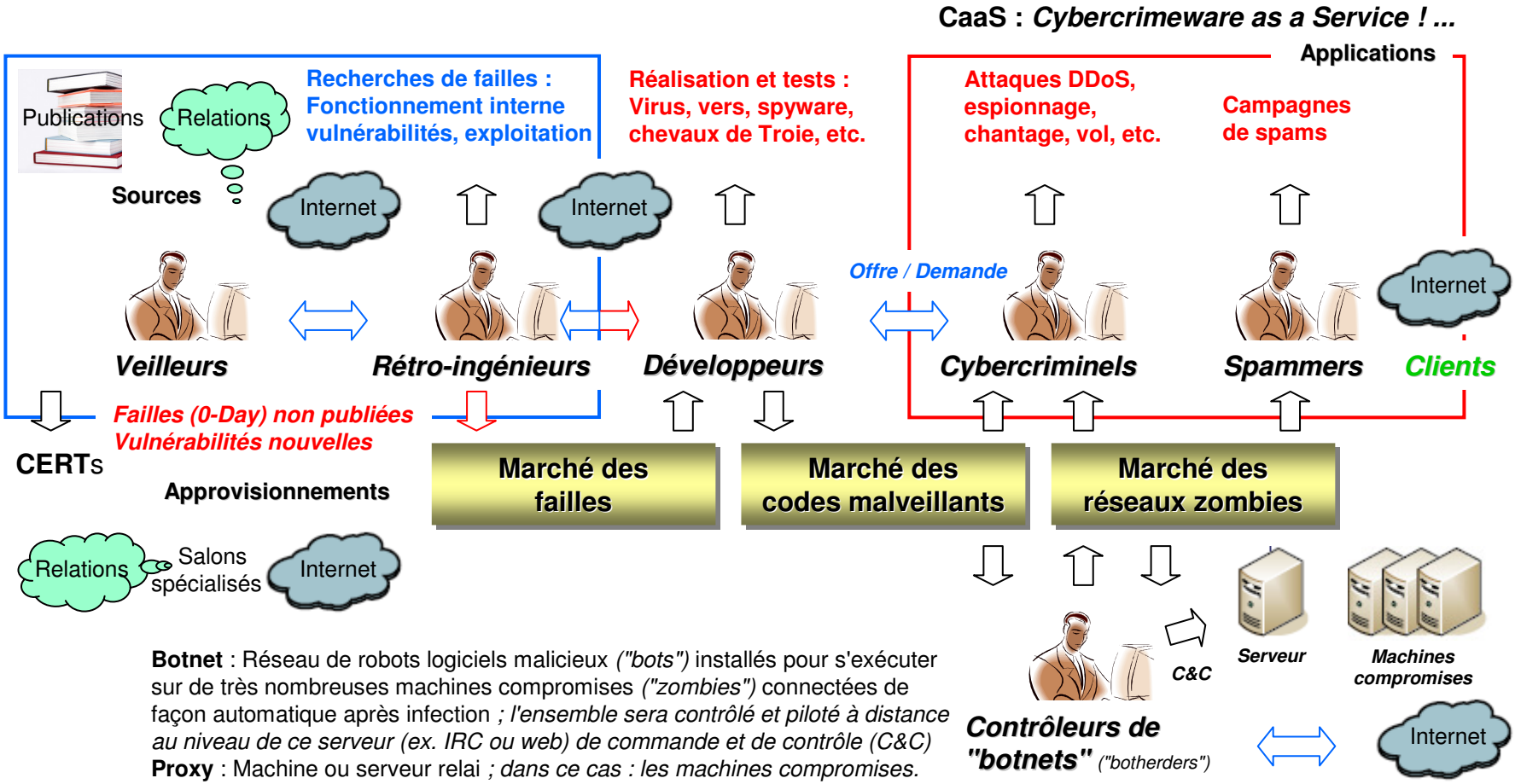
Niveau de sophistication des attaques

Au cours de la période de 1982 à 2000 et au vu de 15 types d'attaques.

Principales attaques et outils utilisés :

Obtention de mots de passe (1), Virus et vers (2), Craquage de mots de passe (3), Exploitation de failles connues (4), Désactivation des fonctions d'audit (5), Portes dérobées et chevaux de Troie (6), Talonnage de sessions (7), Renifleurs et analyseurs de réseaux (8), Mystification d'adresse et de paquets IP (9), Gestion graphique de diagnostics réseaux (11), Dénis de services (DoS) (12), Techniques d'attaques de sites Web (13), Attaques avancées et furtives (14), Début des attaques distribuées, préoccupantes pour les activités en temps réel (15).

... à la cybercriminalité organisée



Botnet : Réseau de robots logiciels malicieux *("bots")* installés pour s'exécuter sur de très nombreuses machines compromises *("zombies")* connectées de façon automatique après infection *; l'ensemble sera contrôlé et piloté à distance au niveau de ce serveur (ex. IRC ou web) de commande et de contrôle (C&C)*
Proxy : Machine ou serveur relai *; dans ce cas : les machines compromises.*

Elle *repose sur une offre et une demande réelles : "botnets" chevaux de Troie vendus et achetés sur eBay, et "proxies" loués pour des campagnes de spams* *(ex. 500 $: 20 millions – 2 semaines)*.

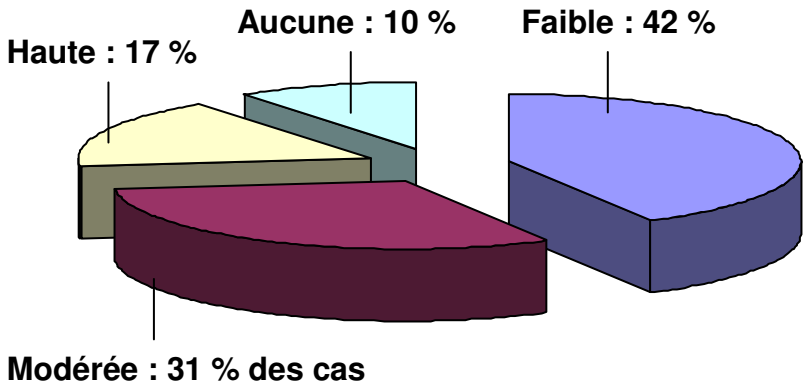
Attaque physique versus logique

- Attaque physique – *Attaque d'une banque*
  - nécessite le contact sinon la proximité pour l'action
  - est limitée à une cible seulement à la fois
  - est immédiatement visible des témoins ou par télésurveillance
  - est associée à des sanctions pénales fortes
  - peut générer un profit matériel et limité au contenu d'un coffre
- Attaque logique – *Cyberattaque*
  - peut être réalisée depuis tout lieu dans le monde
  - est réalisable sur des milliers de cibles à la fois
  - est très discrète et sera découverte tardivement
  - est associée à des sanctions pénales modérées
  - peut générer un profit important et virtuellement transférable

Dans une cyberattaque, l'attaquant est difficile à localiser, du fait de rebonds et de machines compromises en chaîne, et de la découverte tardive ; ce qui la rend avantageuse!

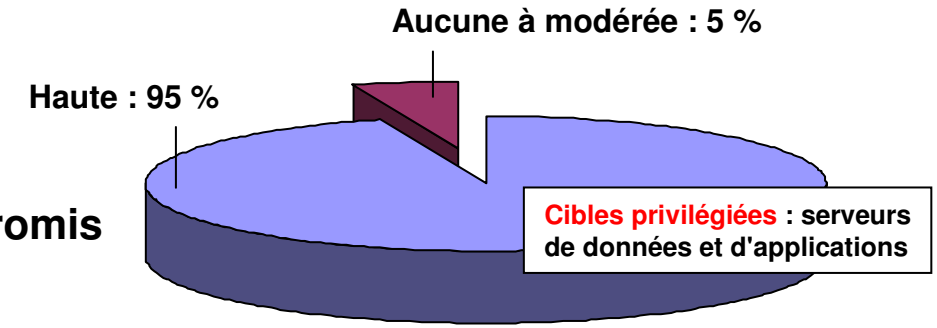
Difficultés liées aux attaques

Rapportées aux attaques menées



Ces attaques sont totalement ciblés pour 28%, dirigées pour 44 %, et au hasard pour 28 %.

Rapportées aux enregistrements compromis

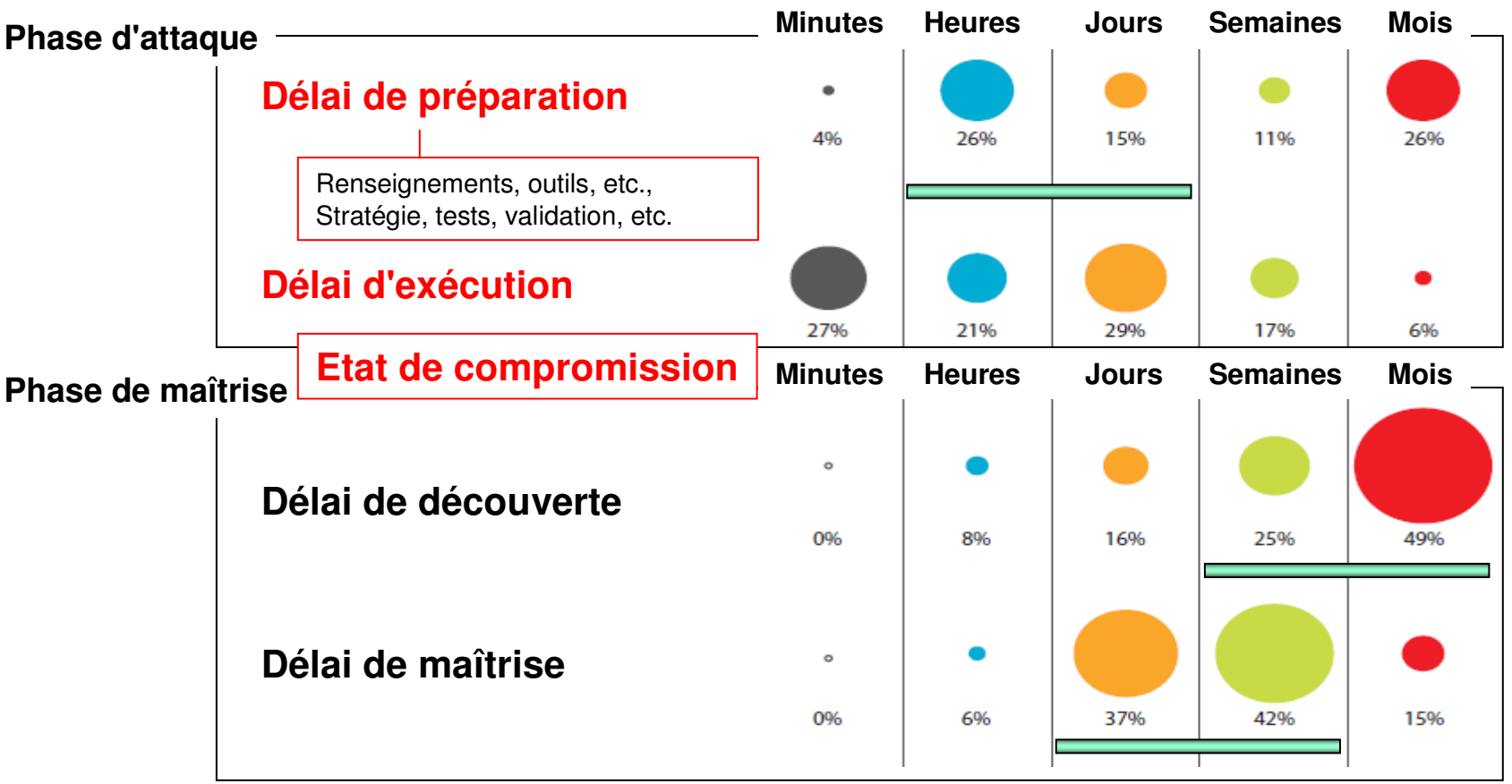


Aucune : L'attaque peut être menée par une utilisateur ordinaire sans ressource particulière.
Faible : Nécessite des connaissances de base, ou des outils automatiques, et de faibles ressources.
Modérée : Nécessite un certain niveau de connaissances, quelques efforts de développement et/ou des ressources significatives.
Haute : Nécessite des connaissances avancées, des développement significatifs et des ressources importantes

Cette relativité est un indicateur de l'environnement, lequel *forme* une chaîne conduisant aux incidents redoutés, au vu d'attaques au 3/4 dirigées ou ciblées.

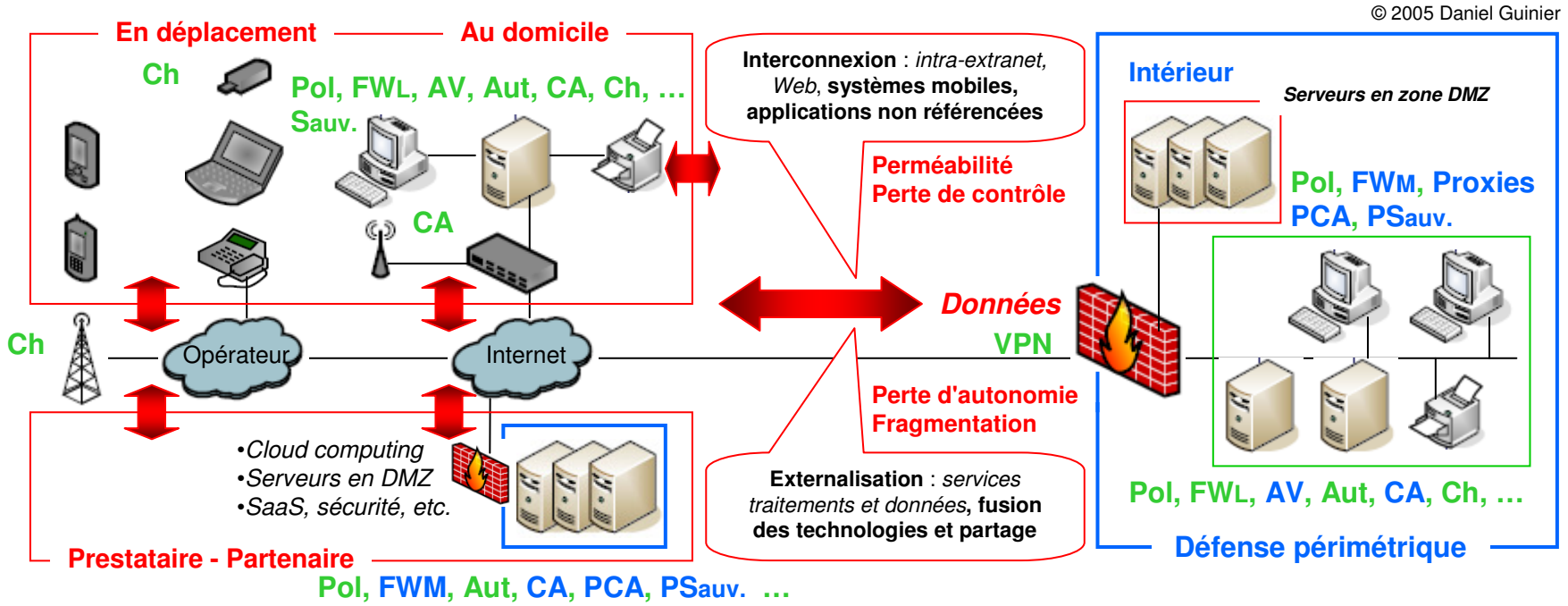
Délais liés à la compromission

Adapté de Verizon (2009) : 2009 Data Breach Investigations Report, *p. 35*



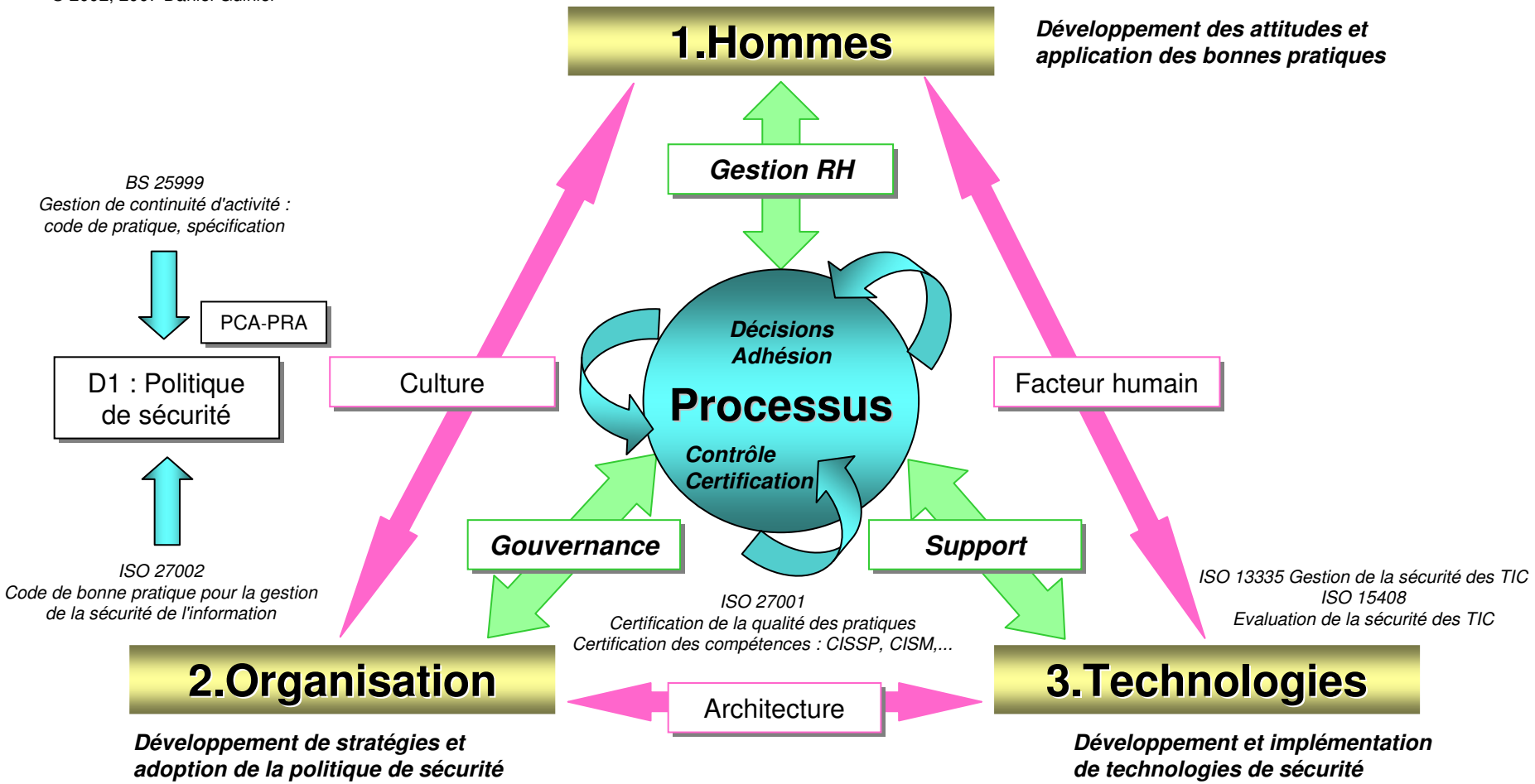
Pour la victime, la découverte et la maîtrise prennent des semaines voire des mois dans 3/4 des cas, alors que pour l'attaquant le délai moyen peut être de l'ordre d'un jour.

Pour une défense en profondeur



Une défense en profondeur par une approche globale est préférable à une forteresse utopique non dépourvue de failles et inadaptée aux nouveaux environnements.

La vision systémique de la sécurité



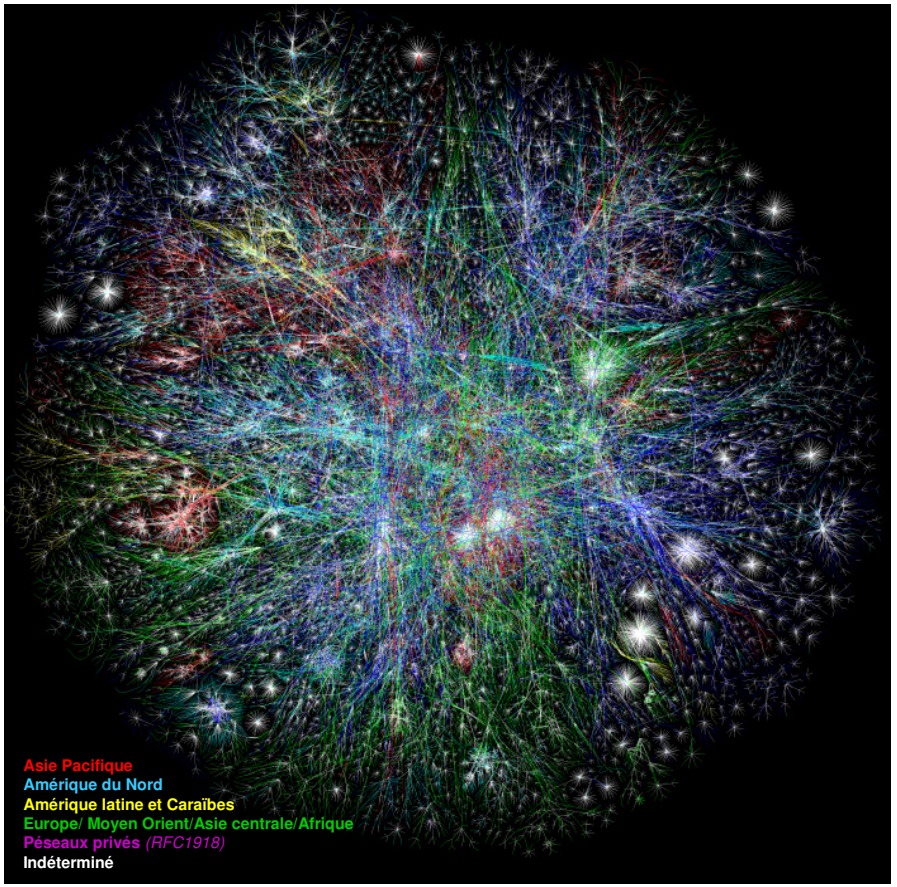
Les trois dimensions sont reliées par des tenseurs dont la régulation est assurée par des processus dynamiques.

Le bouquet final d'un feu d'artifice ...

- Outre l'aspect esthétique

Ce graphe complexe représente une partie des activités Internet, formée ici seulement de 5 millions de nœuds qui représentent les adresses, tandis que les arcs matérialisent les communications.

L'étude participe à la compréhension de la distribution de l'information d'un point à un autre dans diverses directions.



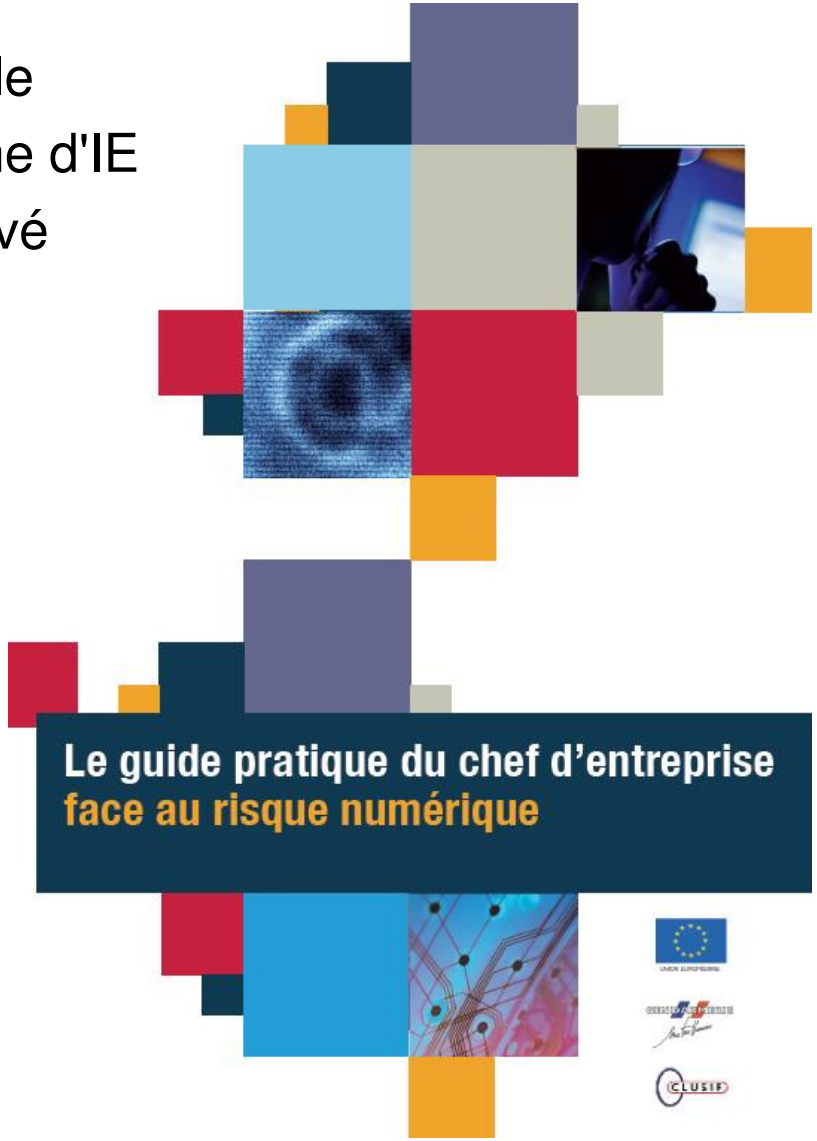
Source : http://www.opte.org

En 2008 : Pour 82 %, les attaquants ont été localisés
En Europe de l'est, Asie de l'Est et Amérique du nord

... formé d'une carte topographique incomplète de l'Internet.

Guide utile à destiné aux entreprises

- Initiative de la gendarmerie nationale
- Inscrit dans le cadre d'une démarche d'IE
- Issu d'une coopération publique-privé
- Destiné à la protection des PME
- Présenté au FIC 2009
- Librement téléchargeable



http://www.fic2009.fr/fr/upload/guide_pratique.pdf

Puis, la crise avait fini par les atteindre directement. L'un perdit son emploi ... un autre claquait des dents et touchait du bois *(Marcel AYME, Maison basse, p. 169).*

Maintenant en pratique avec les tables rondes