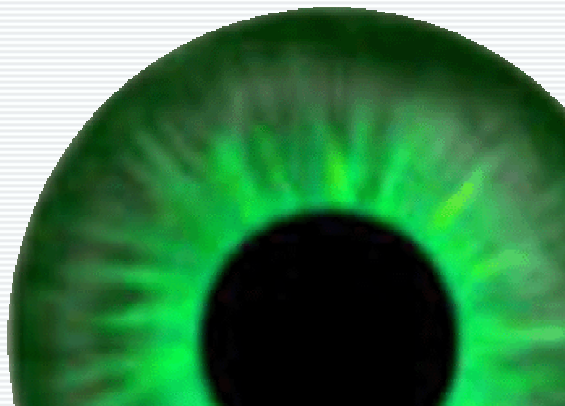
Intelligentzia.net

Stéphane Koch

conseil et formation dans les domaines de la sécurité, l'intelligence économique et de la gestion stratégique de l'information

Société de l'information: entre guérilla et terrorisme, une nouvelle définition des rapports de forces

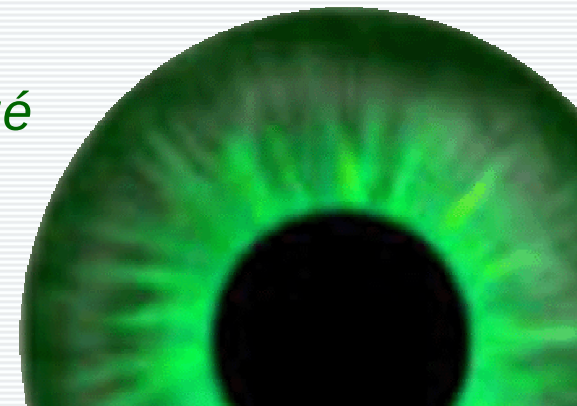
Jeudi 18 mars 2004: XIIIe Symposium international d'histoire et de prospective militaires



Intelligentzia.net

Mon profil:

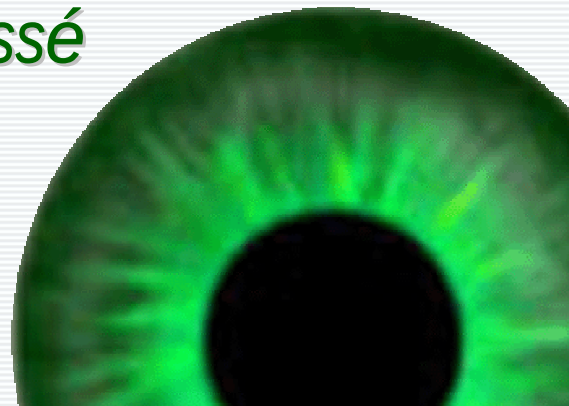
- *Membre du comité scientifique et enseignant au sein de la formation postgrade HES-SO en intelligence économique et veille stratégique*
- *Enseignant et correspondant, Ecole de Guerre Economique, Paris*
- *Enseignant: HEG / SAWI / SPRI / Ecole de Commerce*
- *Dipl. Form. HES-SO, Executive Master of Economic Crime Investigation*
- *Membre du Conseil consultatif de la fondation InfoSurance*
- *Président de l'Internet Society Geneva*
- *Membre du comité du Forum genevois de la sécurité*
- *Membre du comité de la Société Romande de Relations Publiques*



Intelligentzia.net

Contenu de l'intervention

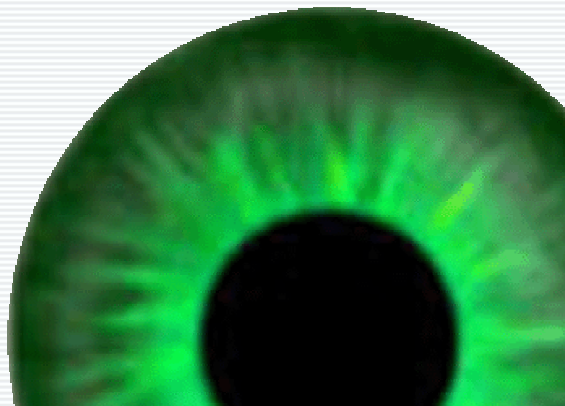
- ⇨ *Sociologie de l'information numérique*
- ⇨ *Répartition des forces & axes stratégiques*
- ⇨ *Axes & outils du Cyber-terrorisme*
- ⇨ *Mode opérationnel & types d'attaques*
- ⇨ *Quelques faits survenus dans le passé*



Intelligentzia.net

Société de l'information:

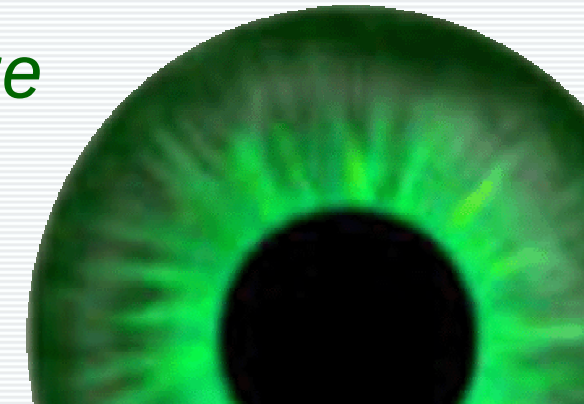
Sociologie de l'information numérique



L'infosphère

- *La circulation de l'information est passée d'un principe d'échange linéaire à un mode d'interaction multidimensionnel.*

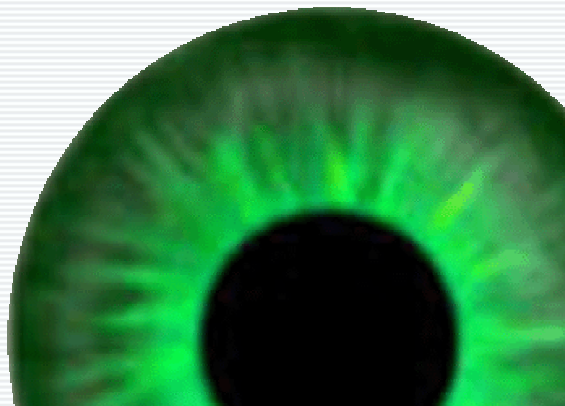
- *Le niveau général des connaissances diminue, créant un fossé technologique au sein même des pays « développés »; affaiblissant d'autant la capacité de discernement nécessaire à la détection précoce des signaux d'alerte*



Un état des lieux de l'information

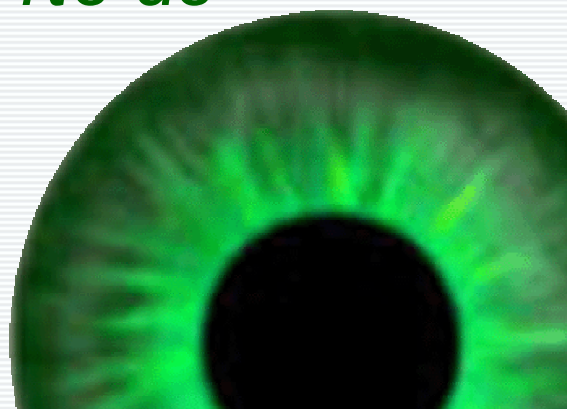
- *Auparavant, les structures classiques de diffusion de l'information reposaient sur des « filtres » de validation établis et contrôlables.*

- *Le Web a généré un système de création et de diffusion de l'information « autodidacte » qui repose principalement sur une dynamique de croyances.*



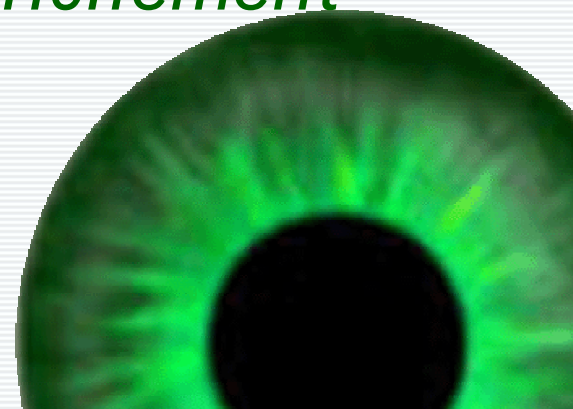
Un état des lieux de l'information

- *Un protocole d'échange unique (TCP/IP) pour des formats multiples, numériquement « déconstruits »*
- *Une capacité à créer et modifier n'importe quel type d'information (texte, image, audio, vidéo)*
- *Aucun contrôle technique de l'intégrité de l'information*



Un état des lieux de l'information

- *De ce fait, on assiste à une augmentation du rapport asymétrique dans la diffusion de la rumeur, par la prédominance de l'émotionnel sur le rationnel.*
- *La réactivité à l'information et la vitesse des échanges qui en résulte, la rend difficilement maîtrisable*



Un terreau favorable

- *La perte de maîtrise entre le potentiel technologique réel des NTIC et la compréhension que l'on en a.*
- *Une conjoncture économique plus difficile, perte de maîtrise de l'environnement technologique*
- *Privatisation et globalisation augmentent le potentiel criminogène intrinsèque présent au sein de l'économie de marché*

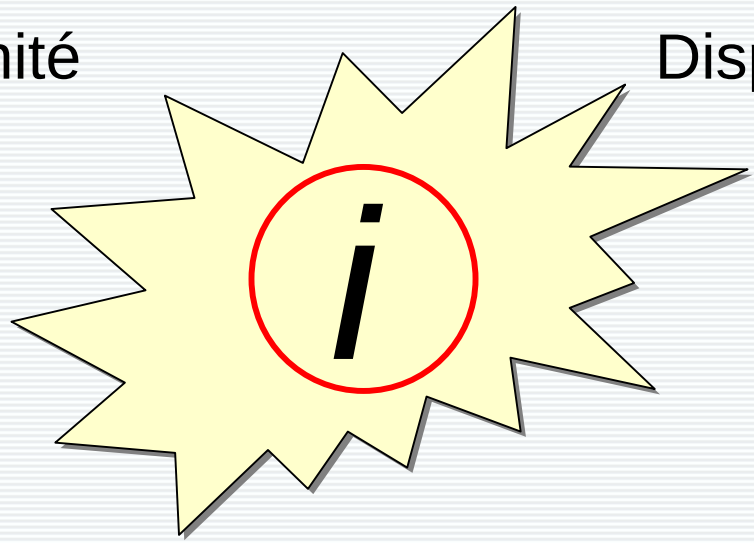
Intelligentzia.net

L'objet informationnel idéal: les variables

production >> émission >> circulation >> réception

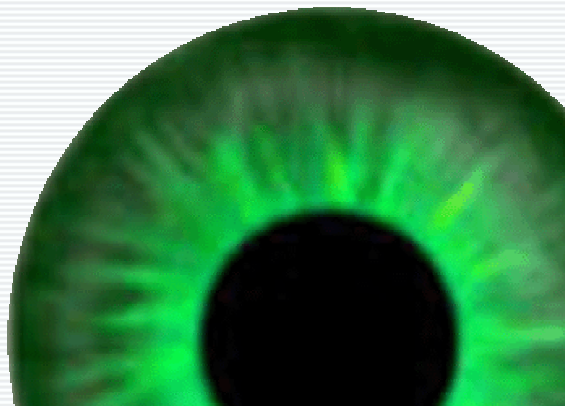
Pérennité

Disponibilité



Crédibilité

Intégrité



Spécificité de l'objet informationnel lors de son interaction avec un environnement humain / NTIC:

- *Le produit d'une croyance, d'une opinion, d'une perception, ou d'une situation*
- *Interagit avec son environnement (positionnement dans les moteurs de recherches, linking et deep linking)*
- *Il créer dynamiquement, en temps réel, de l'information (publication automatique de contenus). Il est donc transformationnel.*

Maslow: la hiérarchie des besoins

L'objet humain: réponse

Comment est-ce que la pyramide des besoins fondamentaux de Maslow peut être interprétée dans l'infosphère?

La réponse humaine à ces besoins fondamentaux est:

- Une faciliter à relayer l'information (hoaxes, virus)
- Une tendance à valider des sources non vérifiées
- L'adhérence quand aux décisions prises ou aux croyances présentes

Intelligentzia.net

Objet humain & informationnel : les variables

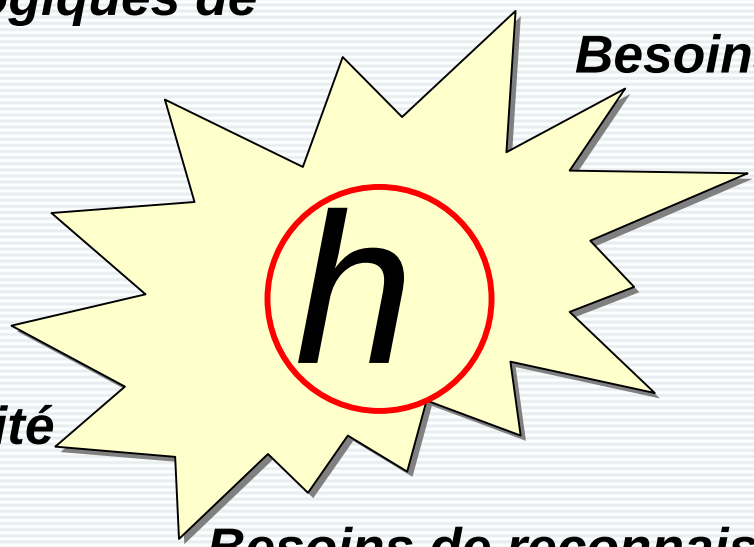
Réception >> traitement >> interprétation >> reformulation

Disponibilité

Besoins physiologiques de base

Besoins d'appartenance

Pérennité

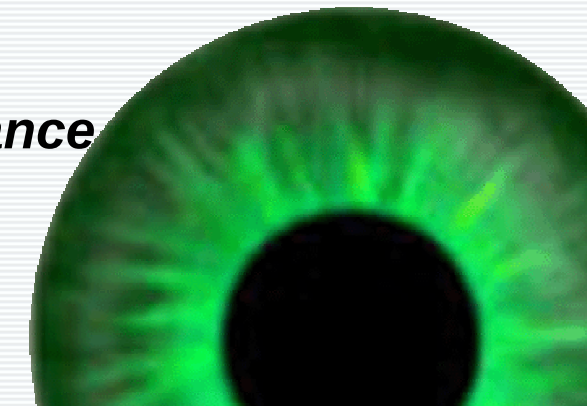


Crédibilité

Besoins de sécurité

Besoins de reconnaissance

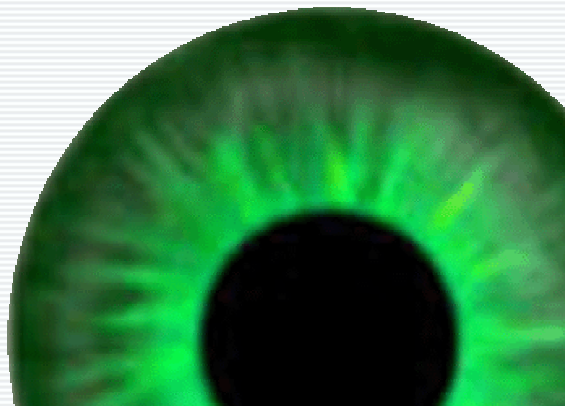
Intégrité

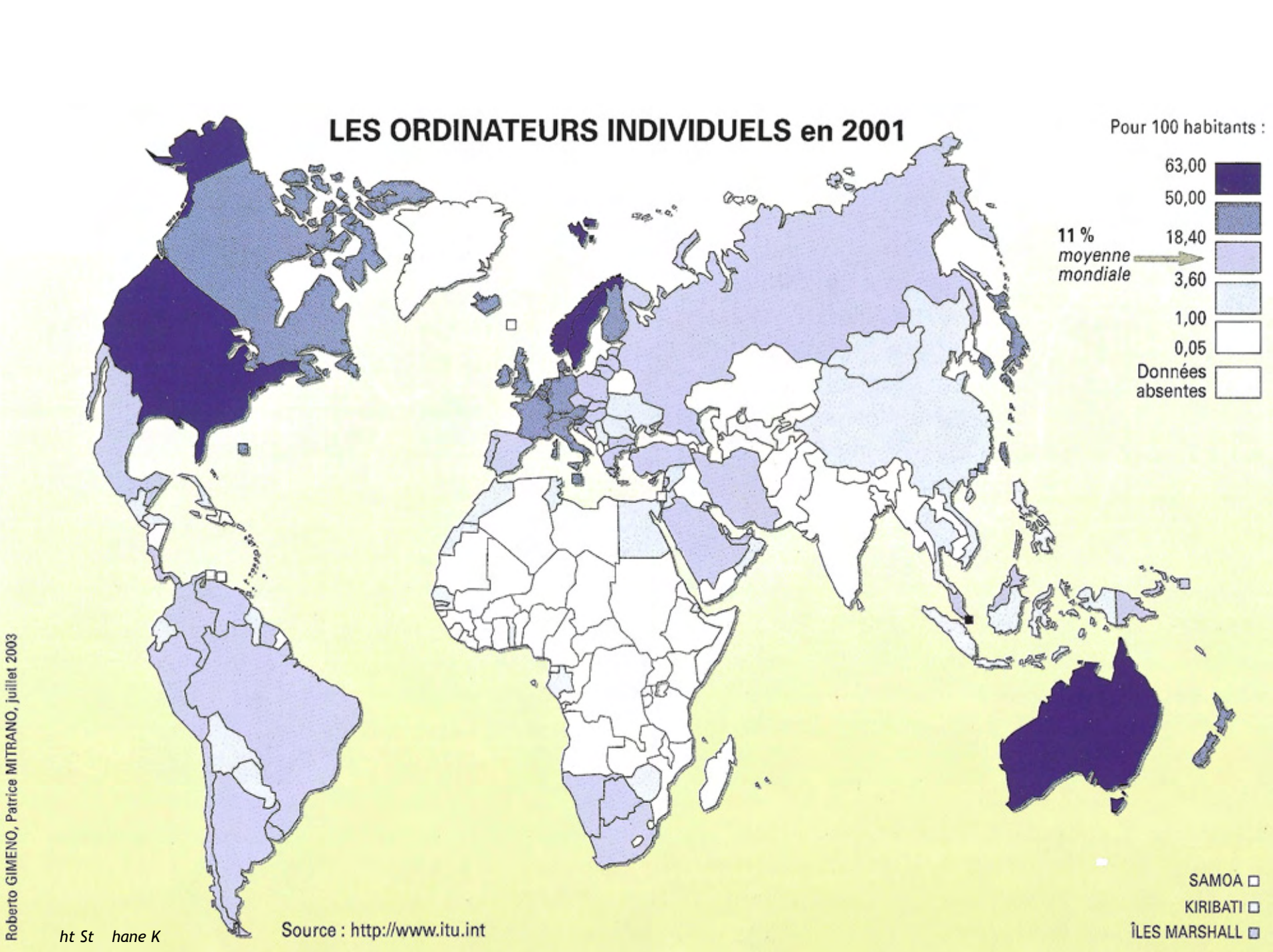


Intelligentzia.net

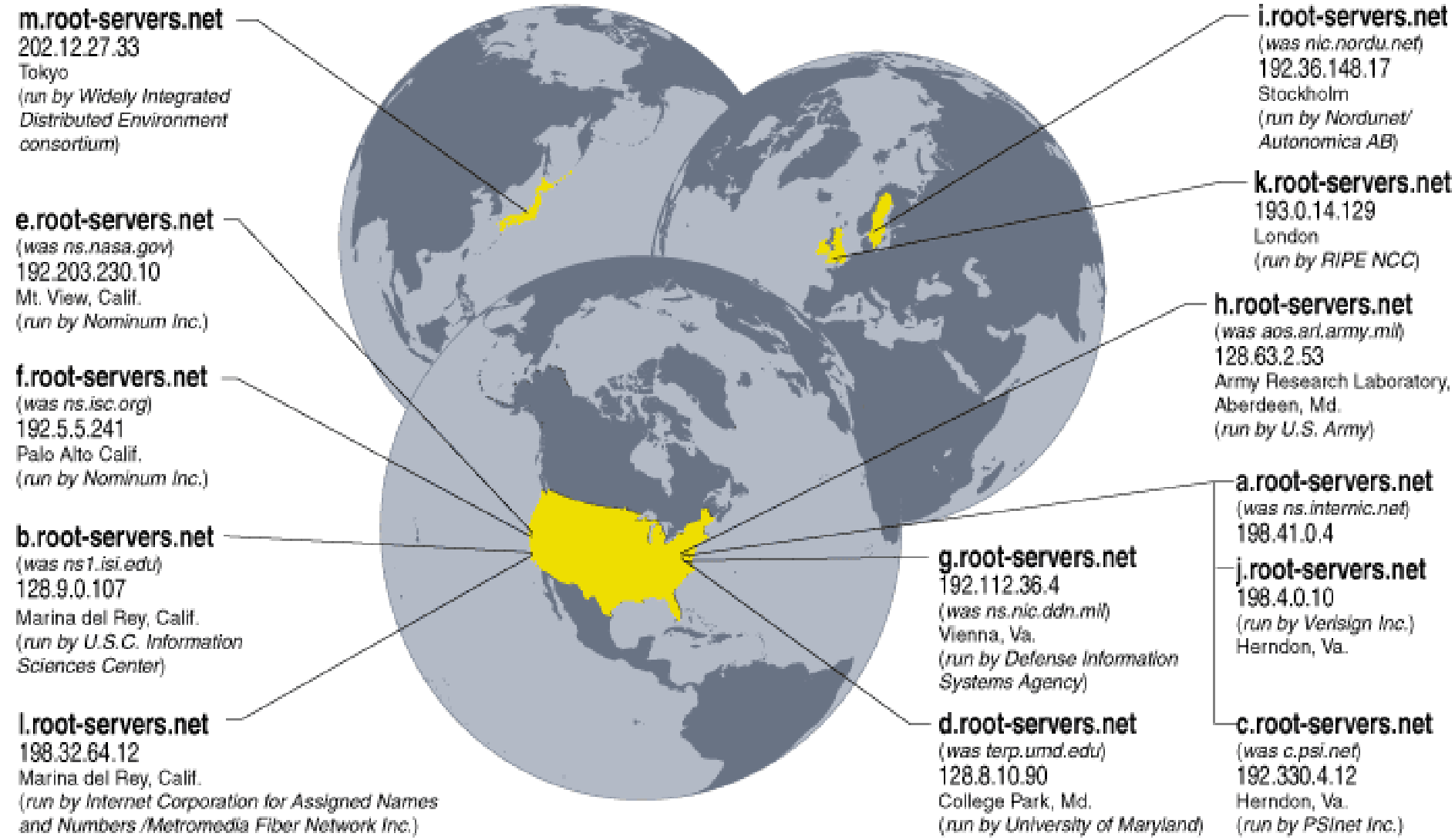
Société de l'information:

Répartition des forces & axes stratégiques




LES ORDINATEURS INDIVIDUELS en 2001
Pour 100 habitants :
63,00
50,00
11 %
moyenne
mondiale
18,40
3,60
1,00
0,05
Données
absentes
Source : http://www.itu.int
SAMOA
KIRIBATI
ÎLES MARSHALL
Roberto GIMENO, Patrice MITRANO, juillet 2003
ht St hane K

«Jusqu'à 2002: 13 serveurs racine, dont 10 au USA. Depuis février 2004, 47 serveurs racine dont 23 aux USA ¦ le serveur racine principal demeure sur territoire US »



ht St hane K

Global Communications Submarine Cable Map 2004

Produced by:

TeleGeography Research

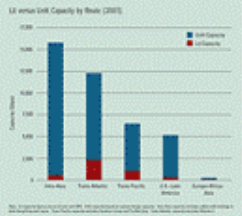
A Research Division of PriMetrica, Inc.

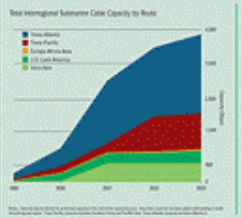
Sponsored by:

Southern Cross Cable Network

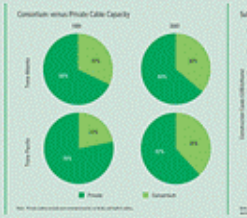
The independent market leader providing fully protected bandwidth in the Asia-Pacific region

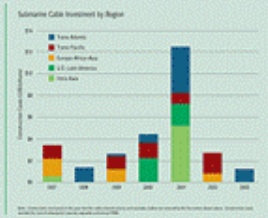
Capacity

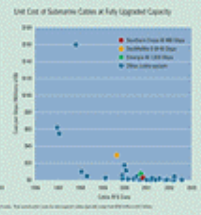


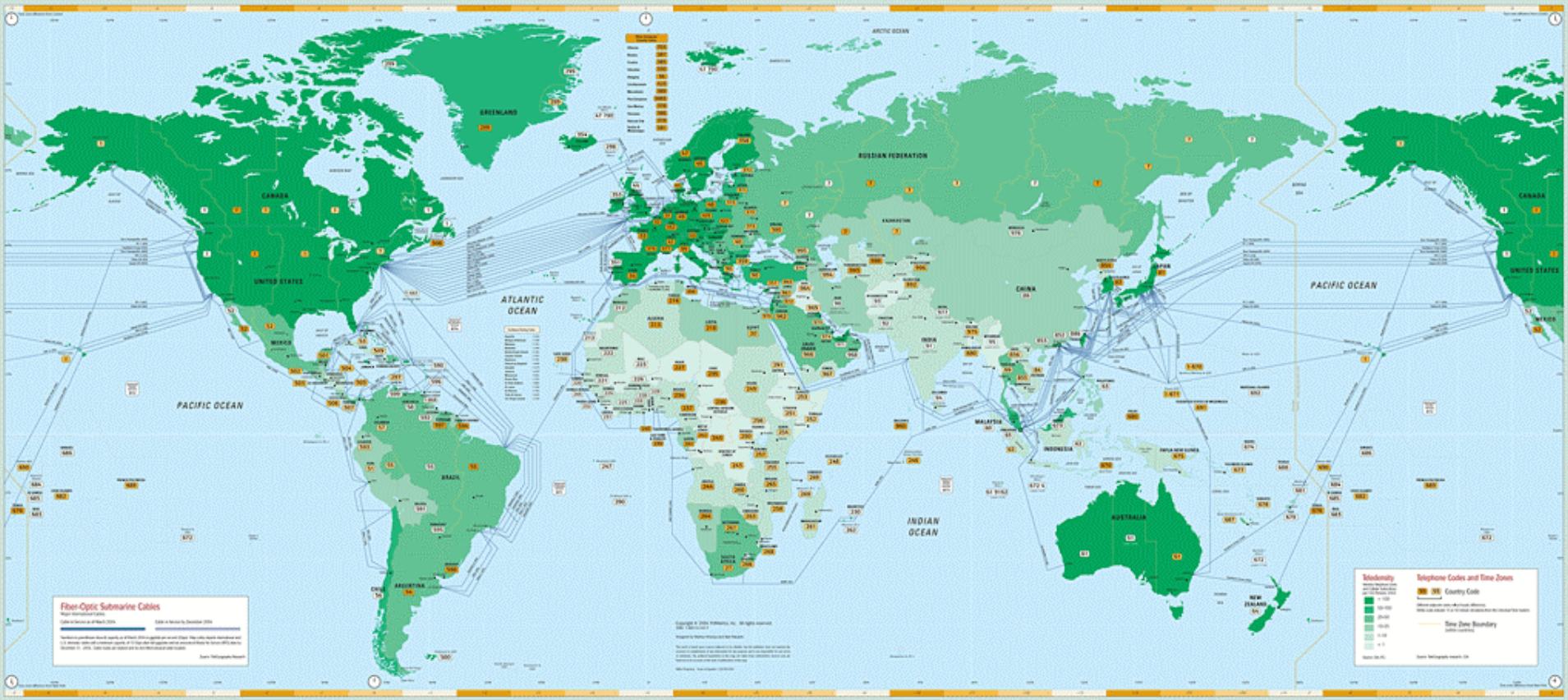


Costs







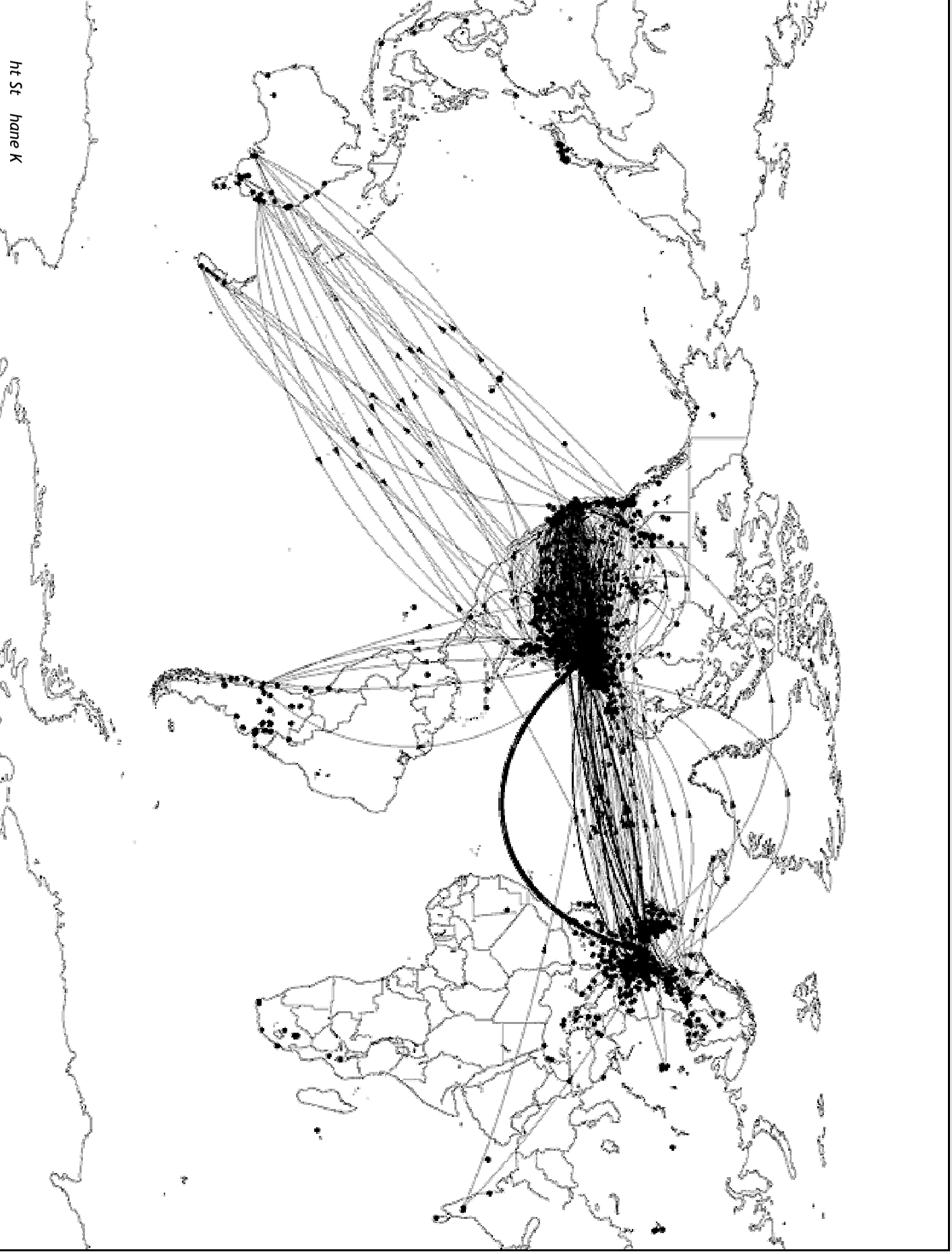


Cable Landing Points

Global Submarine Cable Capacity

Cable Landing Points

ht St hane K



Complete aggregate news flow, worldwide
Line width proportional to directional effective flow volume

DECWRL netmap-2.1 by Brian Reid at Thu May 13 13:49:34 1993
Gall Stereographic Projection, Map center: [15 N, 88 W]

Global Internet Map

First Edition - June 2001

Produced by:

TeleGeography, Inc.

The Source for International Telecom Statistics and Analysis

1325 Massachusetts Ave., NW • Sixth Floor • Washington, DC 20005 • USA

Tel. +1 202 467 0017 • Fax: +1 202 467 0019

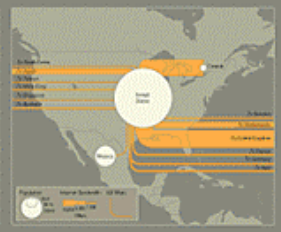
E-mail: info@telegeography.com

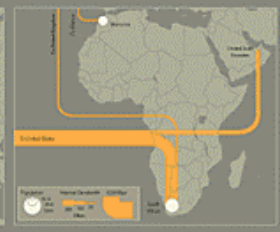
www.telegeography.com

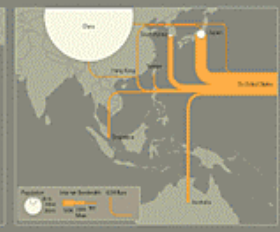
Sponsored by:

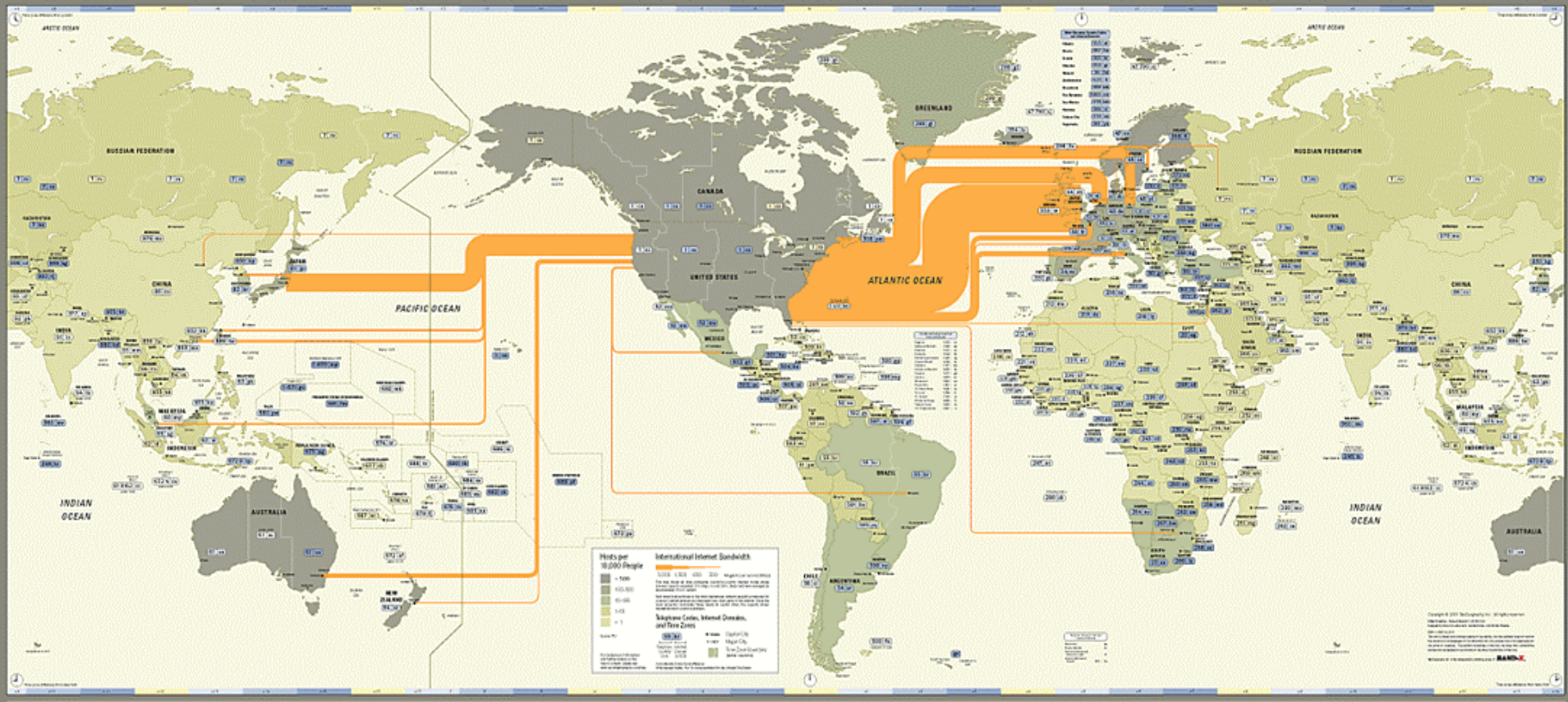
TELIA

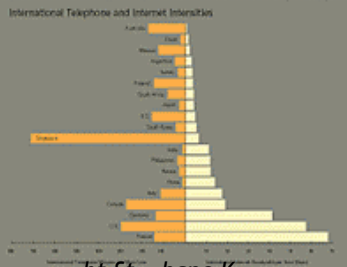
www.Telia.com

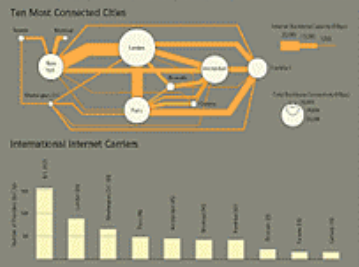


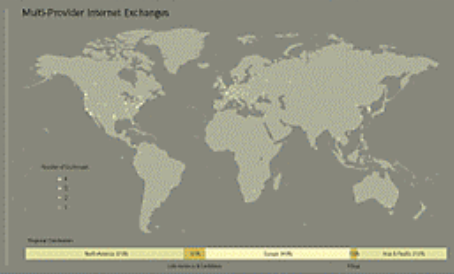


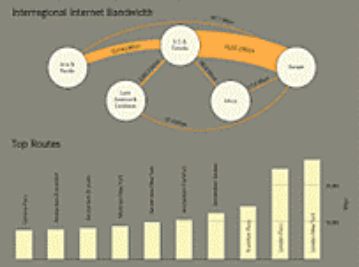


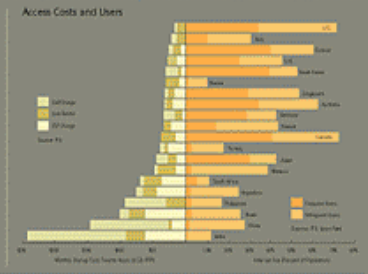












ht St hane K

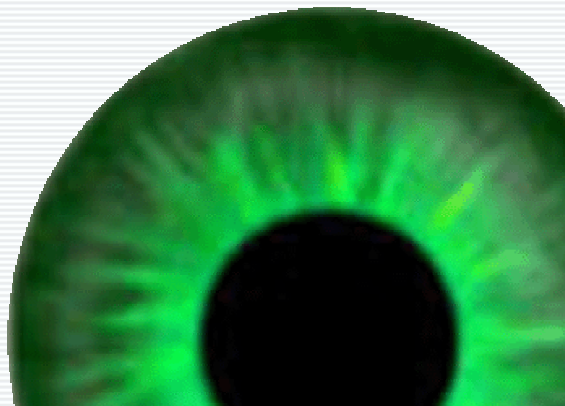
Une certaine dépendance techno-stratégique

- *Les deux tiers des ordinateurs connectés à Internet sont localisés aux Etats-Unis*
- *Les principales liaisons hauts-débits entre les US et l'Europe de l'Ouest passent par Londres*
- *Env. 90% des ordinateurs utilisent Microsoft*
- *Microsoft alimente ses ordinateurs avec des paquets d'information sur lesquels on a aucun contrôle.*
- *80 à 90% du trafic IP passe par les USA*
- *L'ICANN est une société de droit californien*

Intelligentzia.net

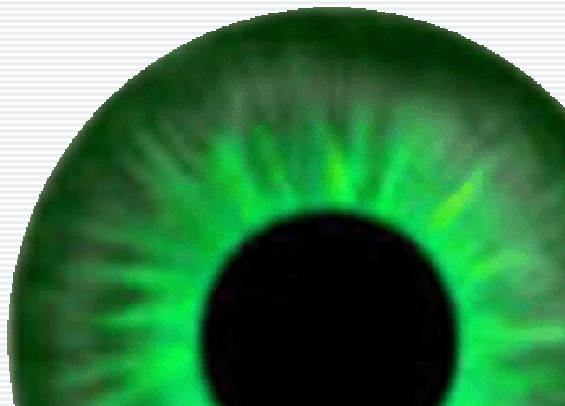
Société de l'information:

Une prédisposition à l'asymétrie des conflits



Redéfinir la notion de temps de paix

Disparition du rapport de force **symétrique** au profit d'une **asymétrie** de celui-ci et d'une **dissymétrie,** au niveau global, des puissances militaires en place

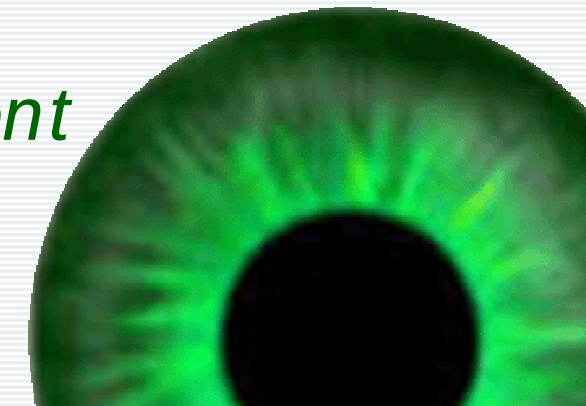


Définition champs classique du conflit

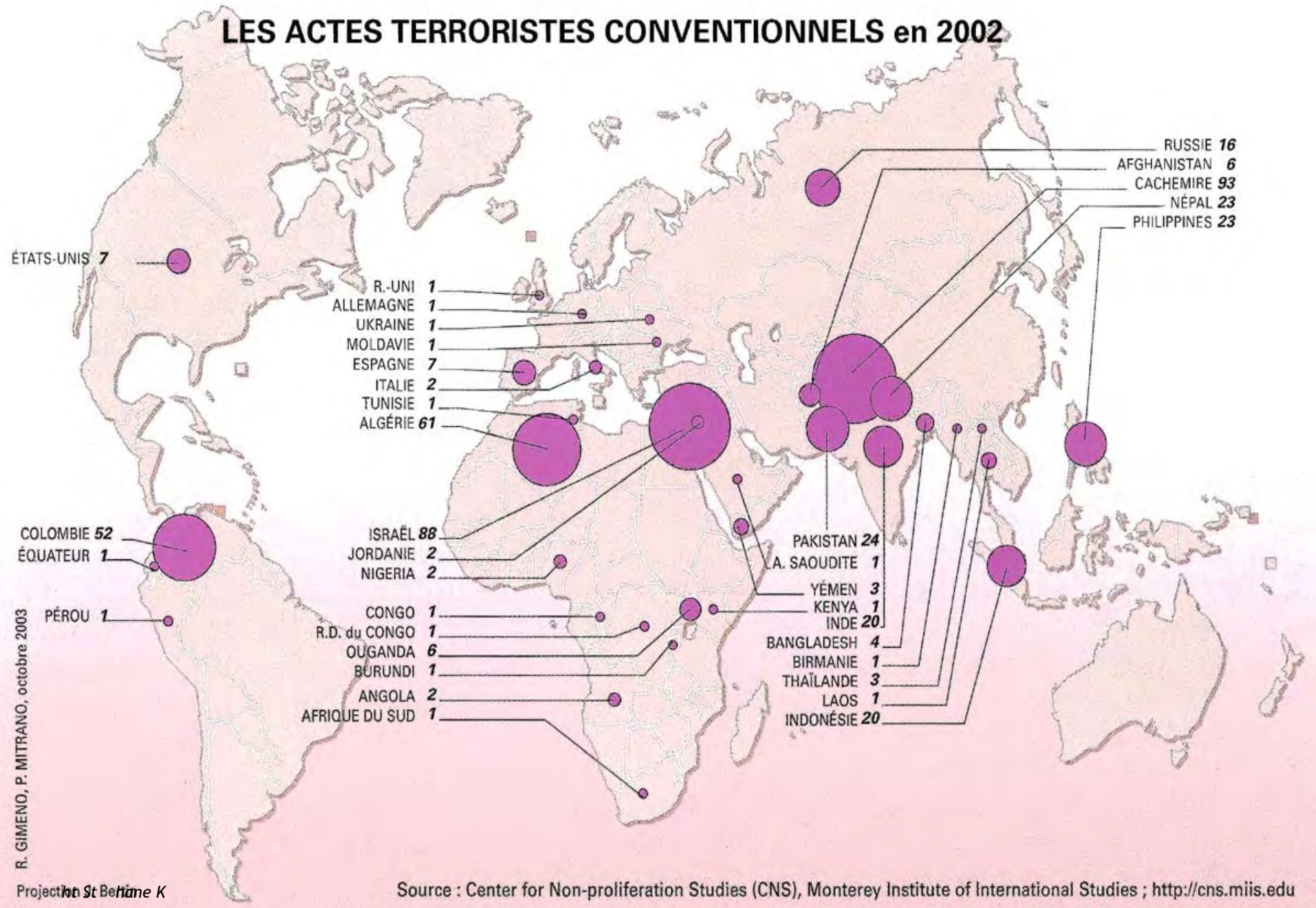
- *Jusqu'à récemment le champs d'opération se limitait à une confrontation sur une zone géographique plus ou moins délimitée.*
- *Le conflit en tant que tel, a « évolué » d'un rapport symétrique des forces militaires en présence, à l'apparition d'actions asymétriques (ex: Somalie & Irak: dispersion des acteurs au sein de la population, sabotages et actions de déstabilisation/terrorisme)*

Définition champs actuels des conflits

- *Actuellement, les conflits s'exportent dans tous les coins de la planète, mais nécessitent une « présence physique » sur le théâtre des opérations*
- *L'interconnexion des réseaux permet, quand à elle, d'agir à distance, de manière délocalisée, derrière les lignes ennemies, tout en restant localisé dans les pays alliés du pays visé.*
- *Les structures de commandement sont de type chaotique ,ce qui permet un fonctionnement autonome.*



LES ACTES TERRORISTES CONVENTIONNELS en 2002



R. GIMENO, P. MITRANO, octobre 2003

Projection de St Bernhame K

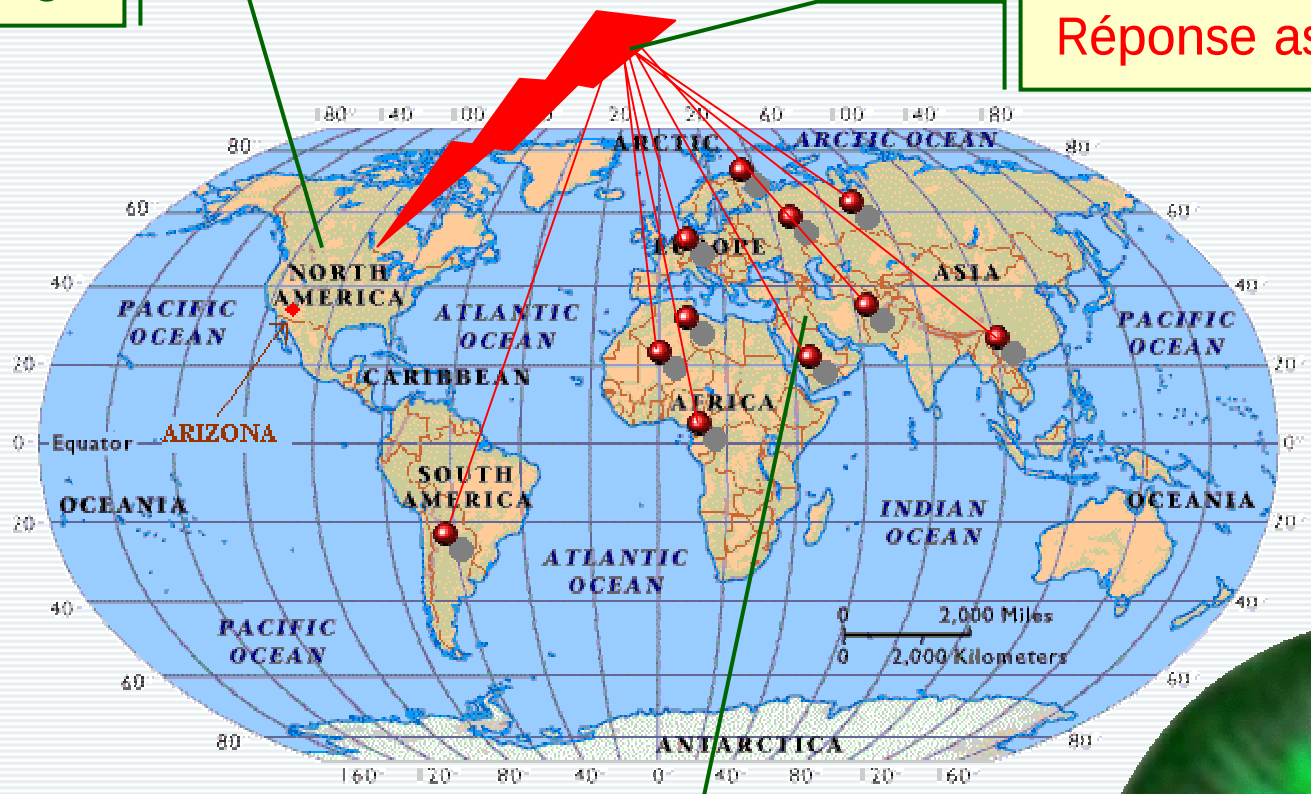
Source : Center for Non-proliferation Studies (CNS), Monterey Institute of International Studies ; http://cns.miis.edu

Intelligentzia.net

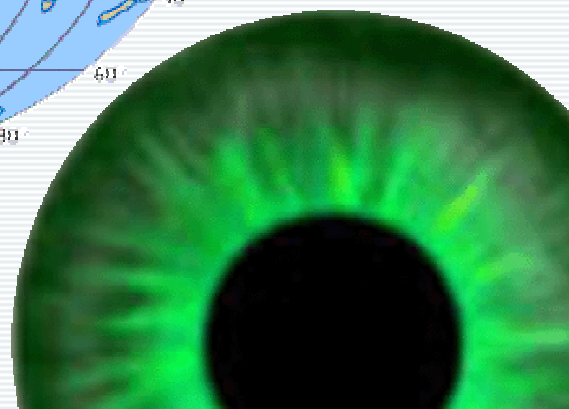
La cyberguerre asymétrique

Etat engagé

Réponse asymétrique

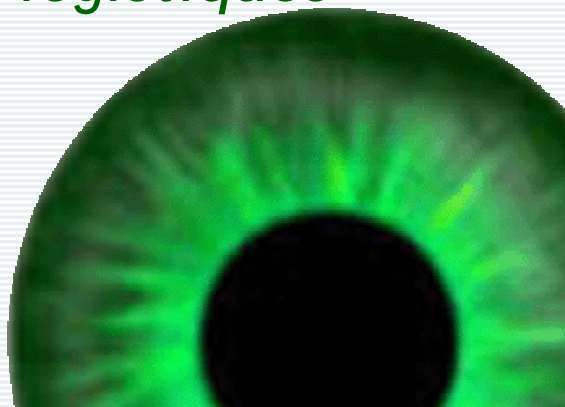


Zone de conflit



Cyberwar: le profil de compétences requis

- *Une éducation technologique (la plupart de l'information est en ligne, des formations informatiques et multimédias poussées existent, et n'éveillent pas de soupçons envers ceux qui les suivent)*
- *Connaissance et maîtrise des ressources logiciels disponibles gratuitement (pour la plupart des outils performants)*
- *Connaissance et utilisation des ressources logistiques disponibles*
  - *Cybercafés*
  - *Réseaux sans fils*
  - *Réseaux universitaires, etc…*



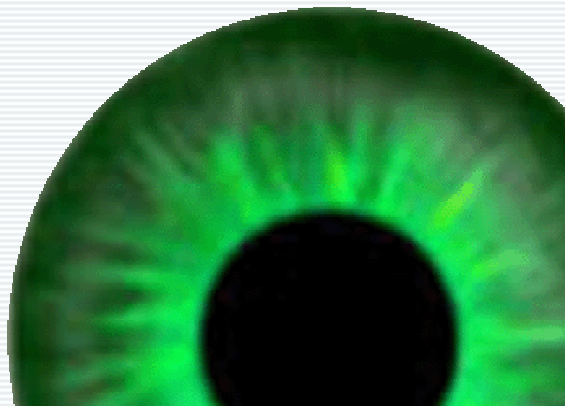
<NetAction>

The Virtual Activist 2.0

A Training Course
developed by Audrie Krause, Michael Stein,
Judi Clark, Theresa Chen, Jasmine Li,
Josh Dimon, Jennifer Kanouse, and Jill Herschman

New! Download NetAction's Virtual Activist Training Reader

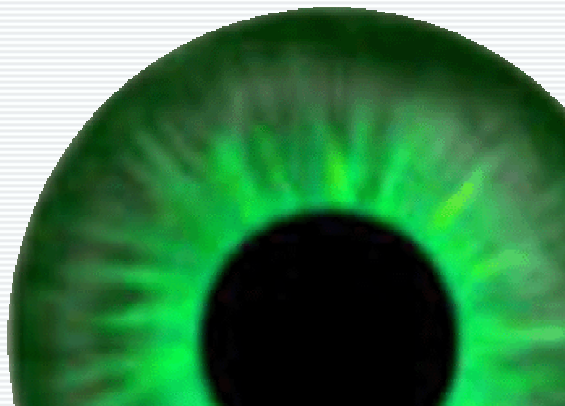
Need more help?



Intelligentzia.net

Société de l'information:

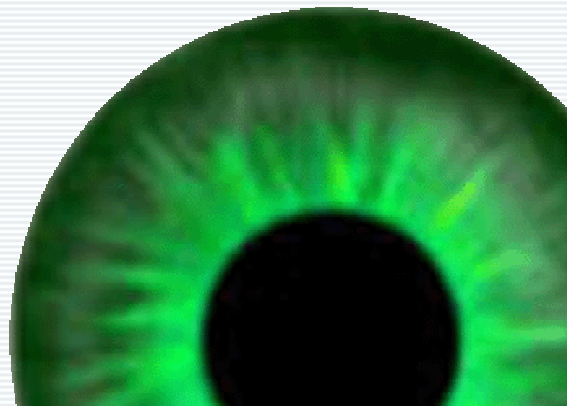
Axes & outils du Cyberterrorism



Intelligentzia.net

L'équipement du parfait « Cyber-Warrior »

- *Un ordinateur portable*
- *Une carte WiFi, et une antenne mobile*
- *Un système d'exploitation – linux ou Microsoft*
- *Une suite logicielle d'anonymisation des données*
- *Un téléphone portable*
- *Un GPS*
- *Un copieur de carte de crédit*



Accès anonymes aux réseaux WiFi ouverts

Communication « one to one » sur plusieurs kilomètres

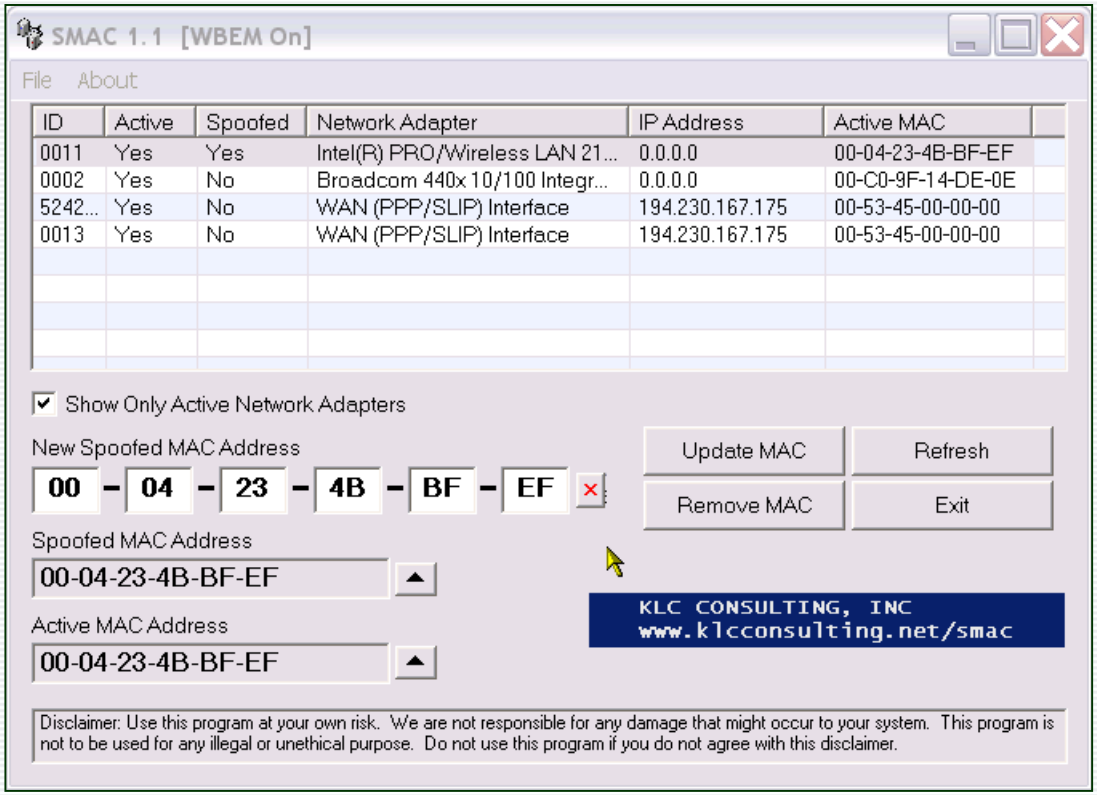
Cryptage des données et camouflage des adresses IP et MAC

Utilisation des NTIC: les pistes de l'anonymat

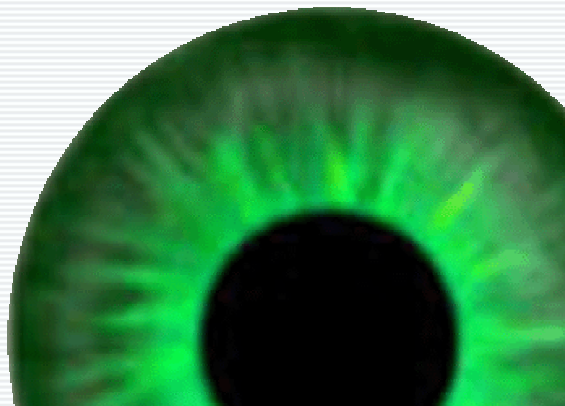
- *« Reverse communication » le principe vise à ce que l'information reste statique plutôt que dynamique pour rendre sa détection plus difficile par les outils de filtrage et d'interception (DCS 1000/carnivore - Echelon).*
- *La stéganographie permet de poster des images dans des forum de discussions (les images sont situées dans la signature du message)*
- *Une approche non conventionnelles du cryptage par la modification des extensions de fichiers ou la segmentation de l'information (les segments d'information sont répartis dans le contenu de plusieurs messages postés dans différents forums de discussions*

Intelligentzia.net

Les outils de l'anonymat: SMAC



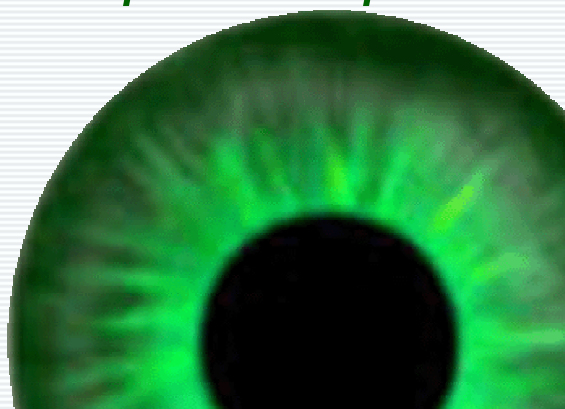
SMAC: ce programme permet de modifier la « MAC address » des cartes réseaux



Intelligentzia.net

Les outils de l'anonymat: les proxies

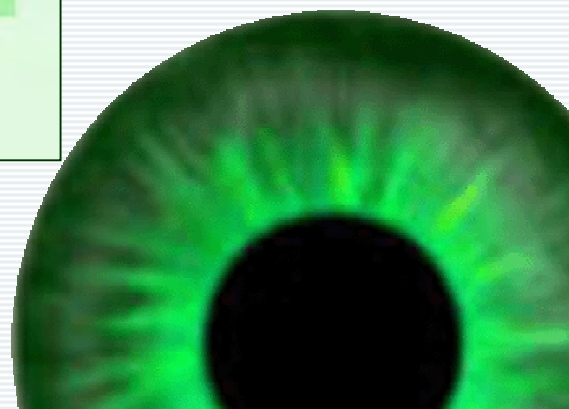
Ces programmes offrent l'anonymat des déplacements sur le Web, ils sont basés sur l'utilisation de serveurs ouverts, ou de ceux dont la sécurité n'est pas adéquate



Intelligentzia.net

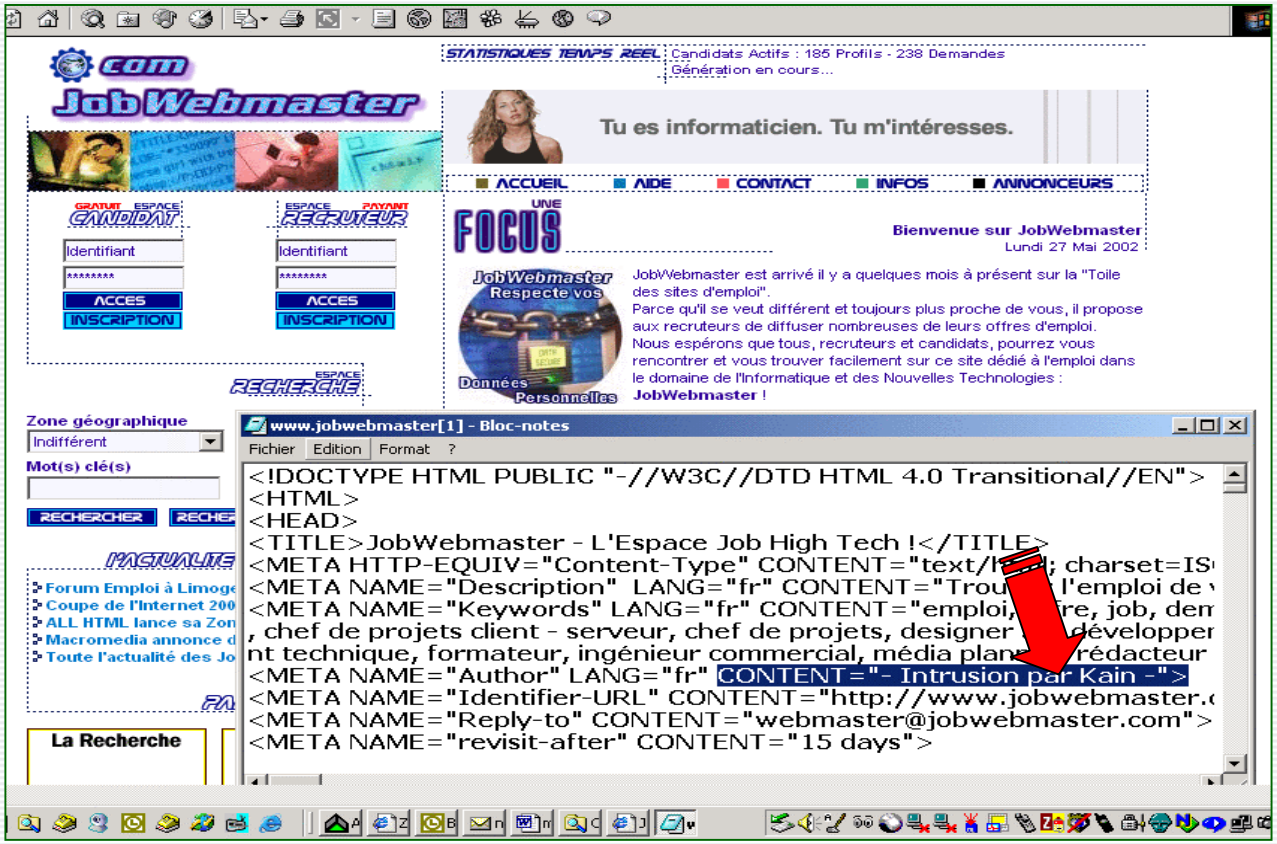
Les outils de l'anonymat: les « Webmail »

« Reverse communication » on utilise les interfaces d'email online « à l'envers » on va communiquer les droits d'accès plutôt que les messages (en combinaison avec l'utilisation d'un proxy)

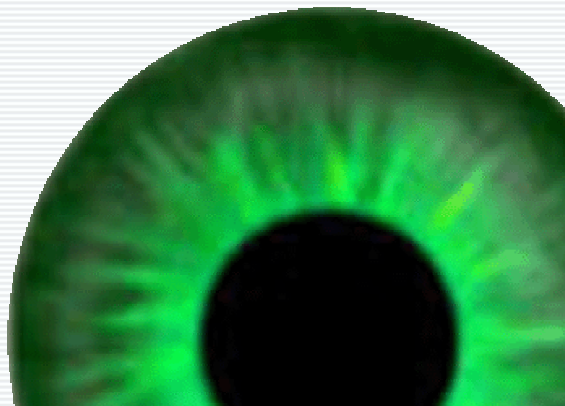


Intelligentzia.net

Les outils de l'anonymat: les page Web

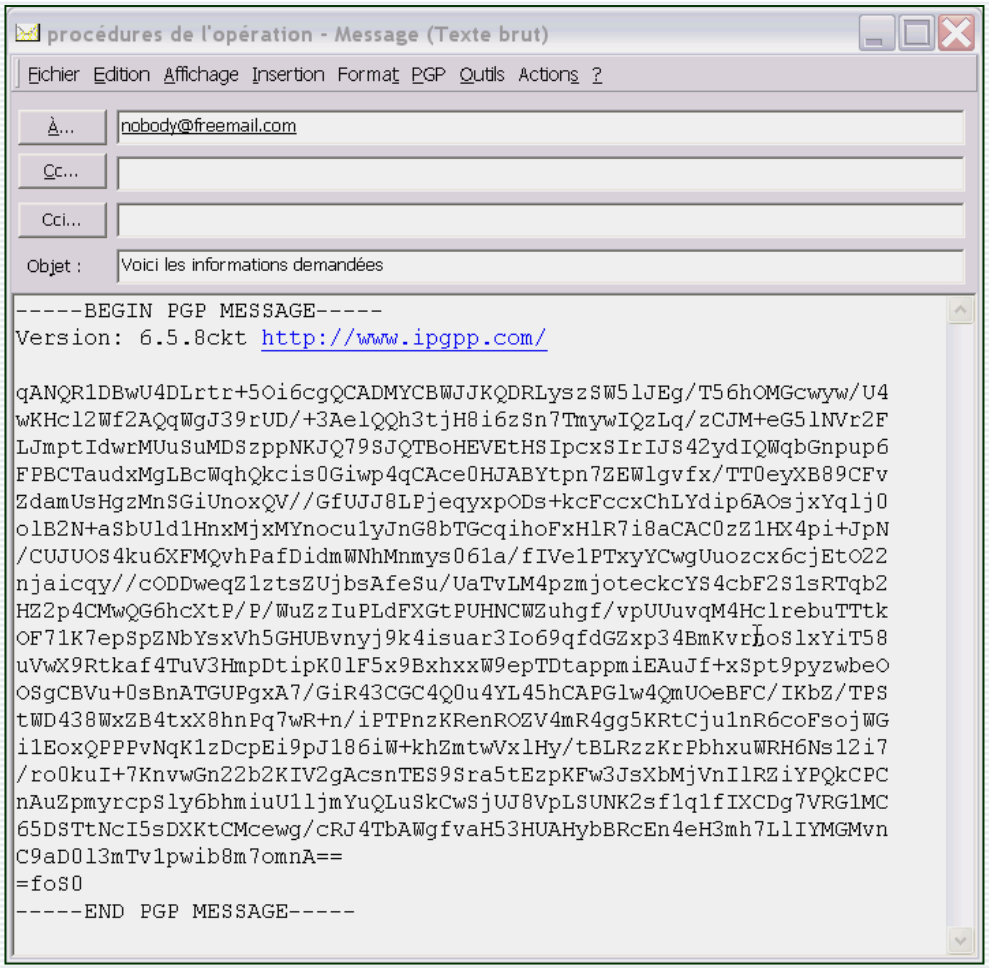


Dissimulation: l'aspect multicouches de l'information

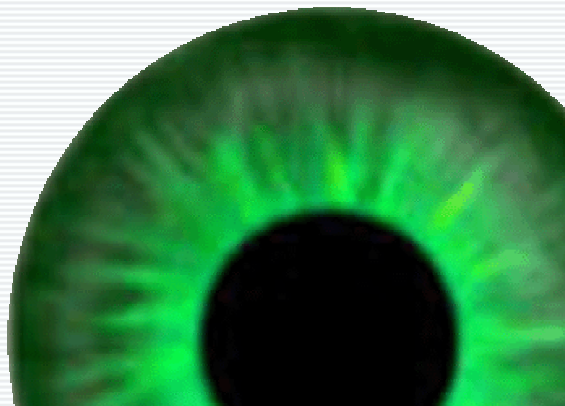


Intelligentzia.net

Les outils de l'anonymat: PGP

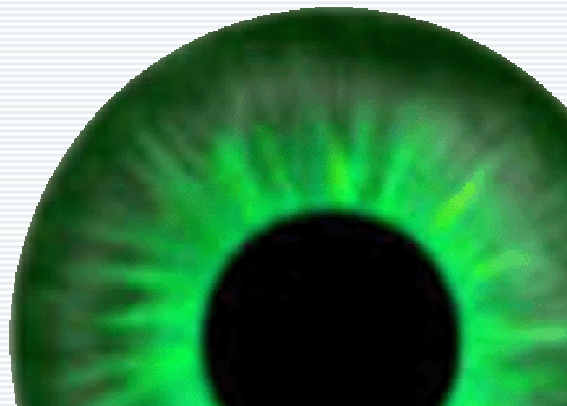


PGP et PGPdisk, offrent un excellent potentiel de dissimulation de l'information



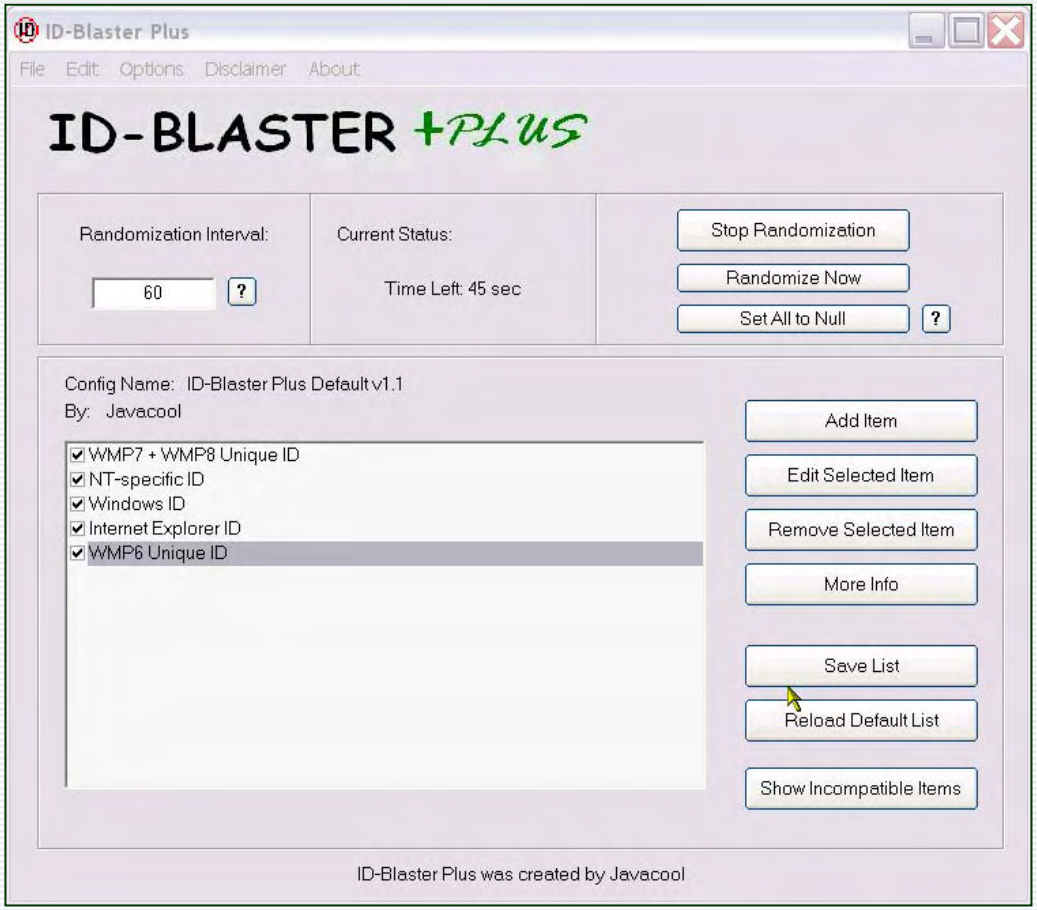
Les outils de l'anonymat: S-Tools

Le programme de stéganographie S-Tools, permet de dissimuler, et chiffrer du texte dans des images (gif, bmp), ainsi que dans du son (Wav)

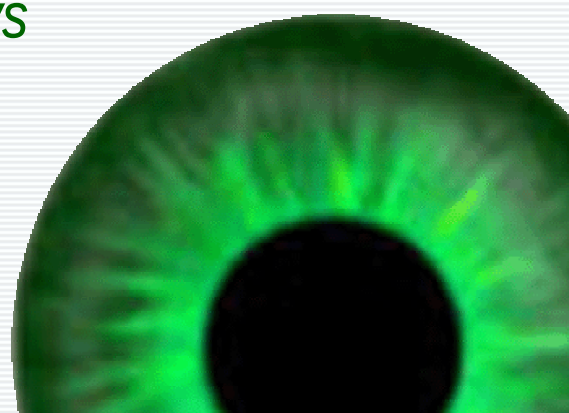


Intelligentzia.net

Les outils de l'anonymat: ID-Balster



Ce programme permet de modifier les différentes informations d'identification présentes sur les systèmes d'exploitation Windows



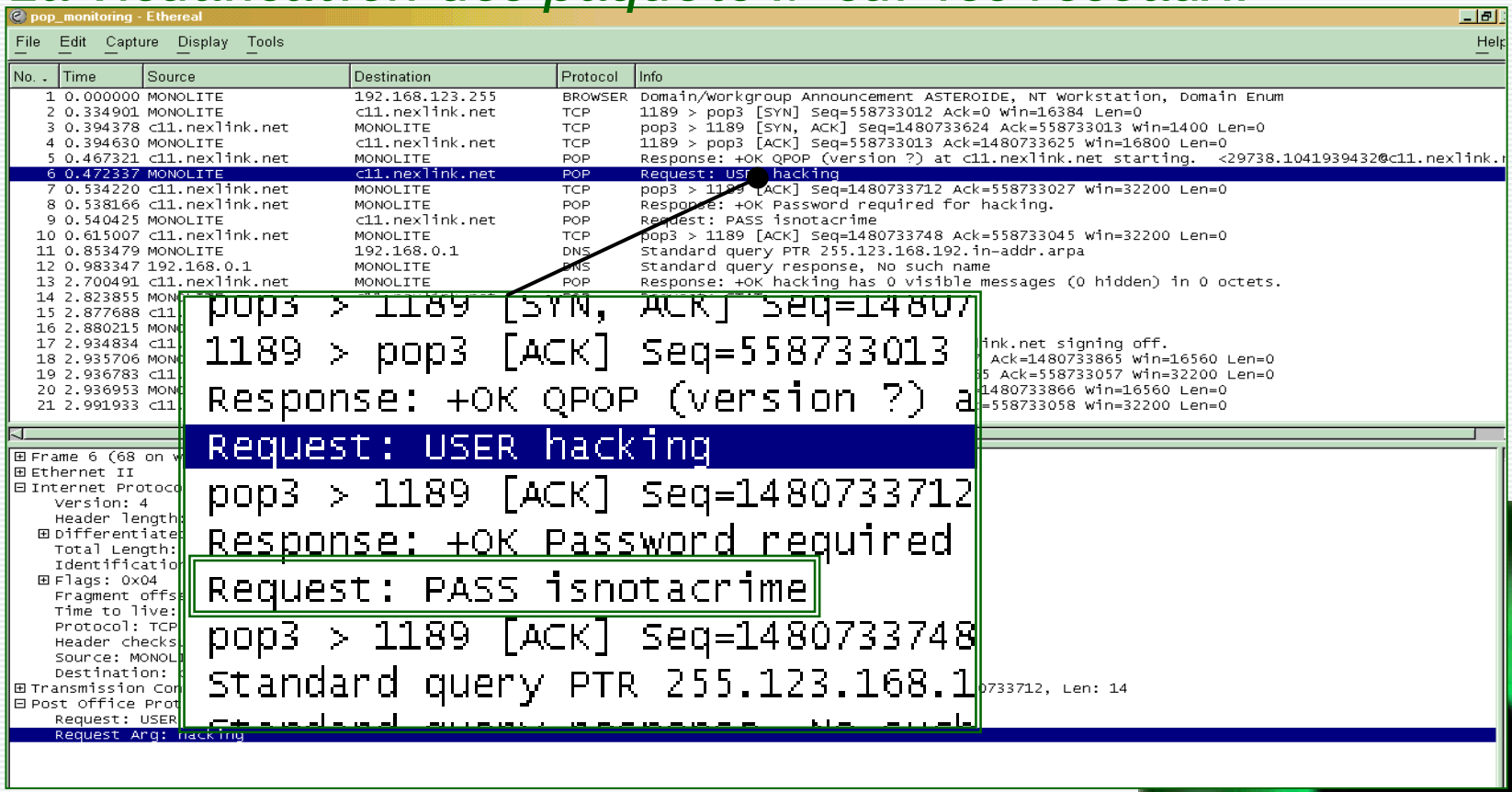
Les outils de l'anonymat: Linux & Co.

Ce système d'exploitation permet d'exploiter un nombre important de fonctionnalités et de programmes développés spécifiquement pour éliminer les traces, s'approprier des réseaux et rester anonyme

Intelligentzia.net

Les outils de l'anonymat:ethereal

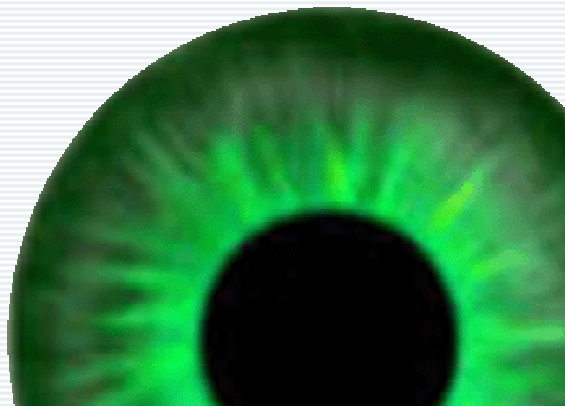
La visualisation des paquets IP sur les réseaux:



Intelligentzia.net

Société de l'information:

Mode opérationnel & types d'attaques



Mode opérationnel: utilisation d'ordinateurs tiers

- *La combinaison entre l'utilisation d'un réseaux sans fil (802.11), d'une connexion ADSL, offre un terrain favorable pour l'installation ou la dépose d'information sur l'ordinateur qui y est relié.*
- *Il existe encore beaucoup d'ordinateurs individuels qui sont pas ou peut protégés. Les diverses options de protections des réseaux 802.11 comme le « WEP » ou la reconnaissance de la « Mac address » ne sont pas assez fiable.*
- *La taille importante des disques durs rend difficile la détection de contenus supplémentaires par des personnes possédant peut de connaissances techniques*

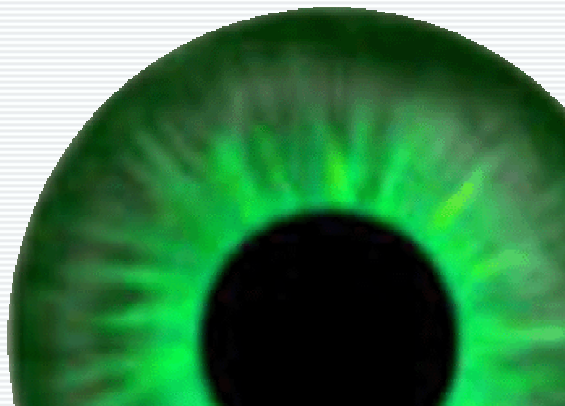
Mode opératoire potentiel, du mode de fonctionnement de cellules (cyber)terroristes

- *Un ensemble de cellules terroristes se fond dans la population, au niveau de chacune de ses composantes individuelles (mimétisme culturel et comportemental).*
- *Les contacts entre les éléments composant la cellule sont réduits au minimum et régis par des procédures préétablies (cryptage et stéganographie, Wireless)*
- *Lorsque l'une des cellules doit être activée, elle ravive ses « éléments » par le biais du réseau. Chaque cellule est autonome, les médias servant de centralisation de l'information lors des diverses actions*

Intelligentzia.net

Mode opérationnel au niveau de la collecte et du traitement de l'information

- *Echanges des données collectées par mode crypté ou sur des boîtes aux lettres électroniques statiques - Pas de nécessité de contact grâce aux réseaux sans fils*
- *Utilisation des méthodes de piratage, Installation de Chevaux de Troie, keylogger*
- *Exploitation des faiblesses humaines par « Social engineering »*
- *Exploitation des sources ouvertes*
- *Exploitation des données accessibles commercialement (ex:>>)*




SPACE
IMAGING
Madrid Atocha
1st Landmark

Les armes asymétrique

Internet et le Web n'ont pas été créé, à la base, pour répondre à une problématique de sécurité au niveau des données transportées. On peut aisément falsifier le protocole IP

IP Hijacking – IP telephony

IP Spoofing – crypto

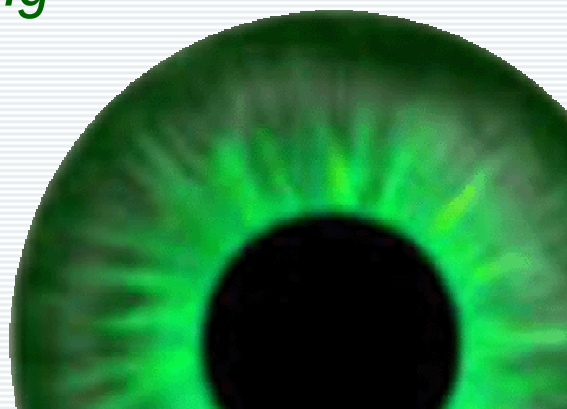
IP Sniffing – steganography

forget Web site – Email bombing

Email spoofing – backdors

Brute force – Open relay

DoS – virus

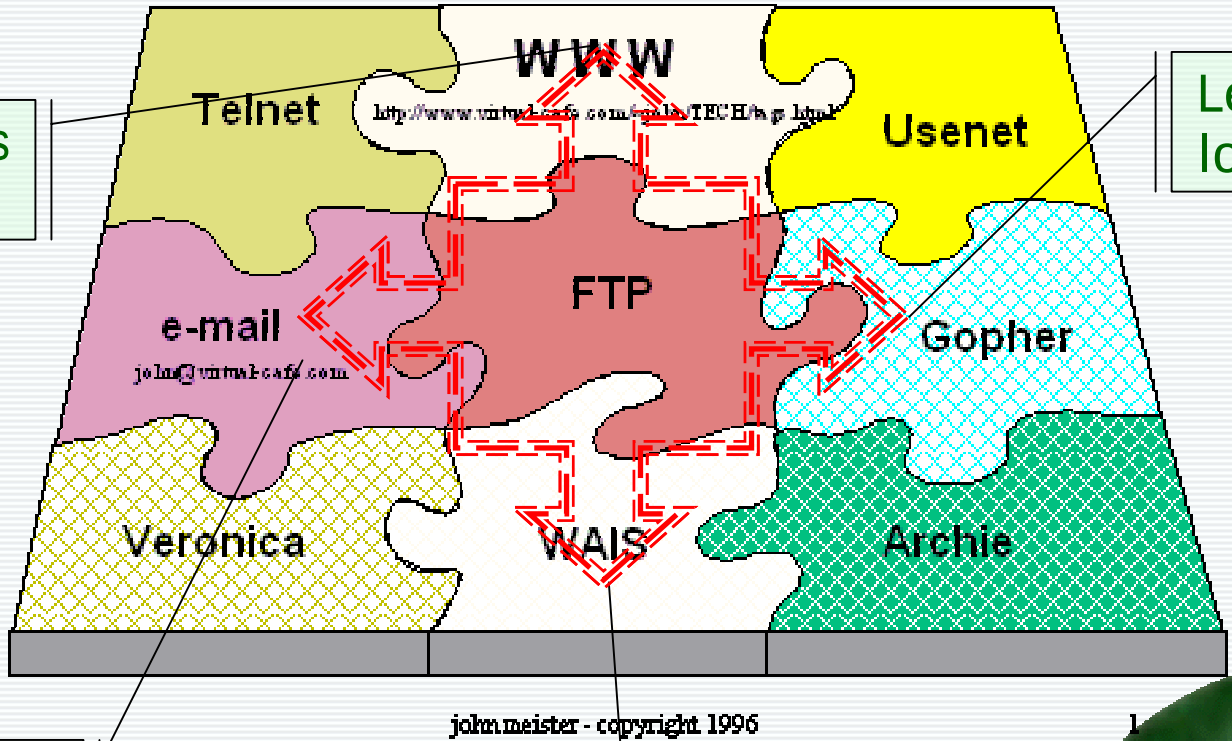


Intelligentzia.net

Stratégie du numérique: typologie des attaques

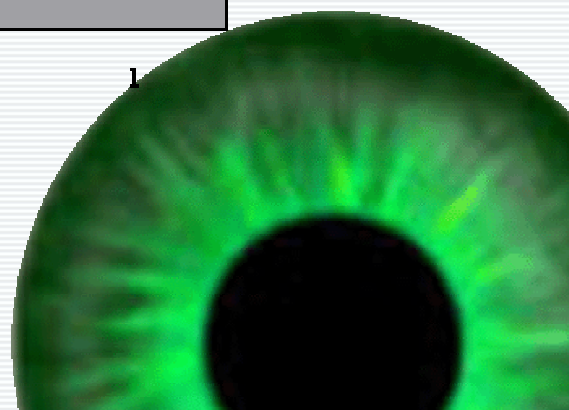
Les attaques techniques

Les attaques logiques



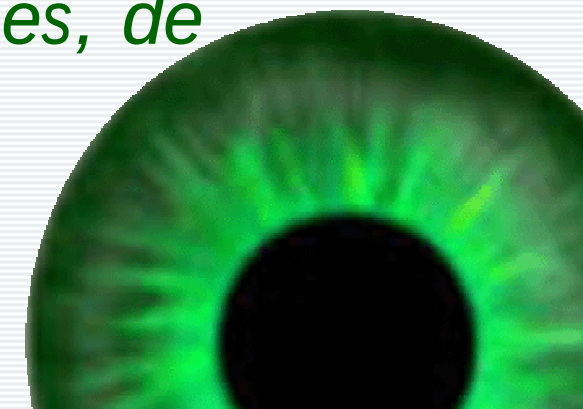
Les attaques psychologiques

Les attaques dynamiques



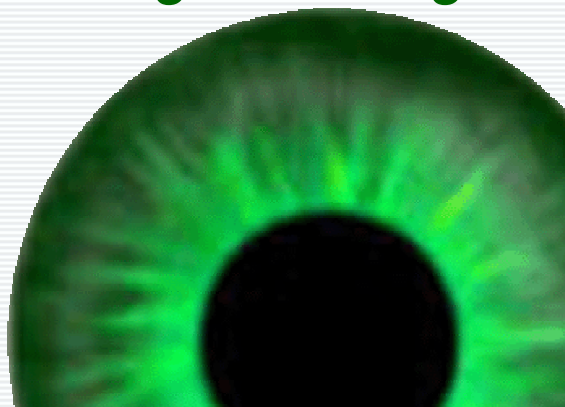
Les attaques de type « techniques » :

- *Elles visent les infrastructures tels que les Serveurs DNS, les serveurs réseaux, les routeurs, les infrastructures de transport de l'énergie, les installations gérées à distance, les infrastructure de gestion de la distribution de l'énergie, les processus d'automatisation de tâches, de surveillances ou de contrôles*



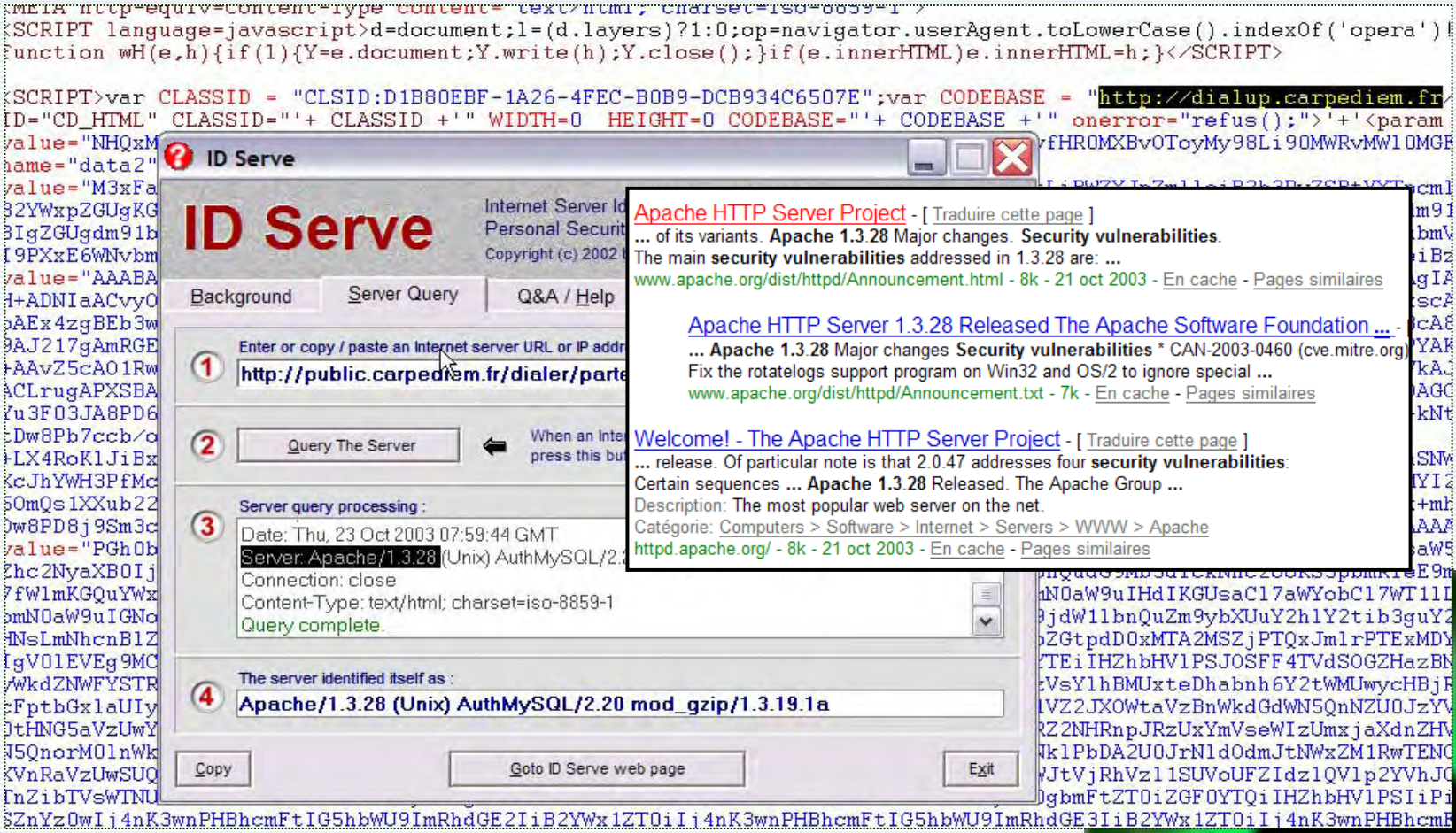
Les attaques de type « logiques »

- *intrusion dans les ordinateurs d'entreprises ou de particuliers (hommes politiques, militaires), installation de chevaux de Troies, effacement, vols, altération des données. Collecte d'information à haute valeur ajoutée. Utilisation de la couche Web, mail bombing, denial of service, social engineering, usurpation d'identités, utilisation de la documentation des failles de sécurité et autres « exploits »*



Intelligentzia.net

Exemple: préparation d'une attaque de type «logiques



Exemple d'outils

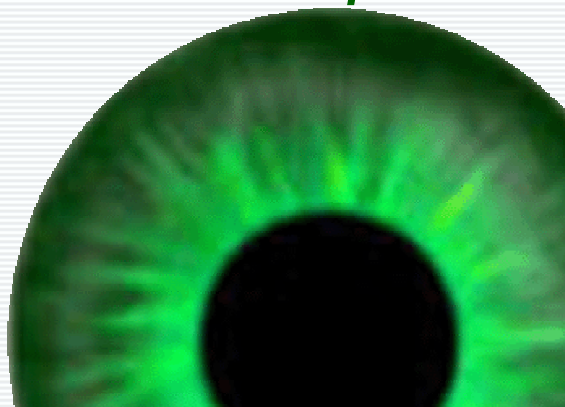
http://www.libellules.ch/anti-dialer/fauletricks.html

Intelligentzia.net

Fonctionnement du Keylogger

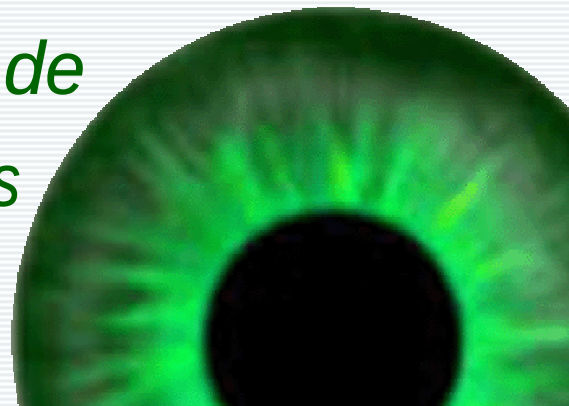
Les attaques de type « dynamiques »

- *utilisation de virus de type « worm »,pour que les éléments d'attaque se servent des ressources du Net/Web pour s'auto-propager. Utilisation de ressources statiques ayant une action dynamique (activ x, console Java, failles des navigateurs). Utilisation des failles humaines, liées au manque de connaissances technologiques (faux site, faux email, etc…)*



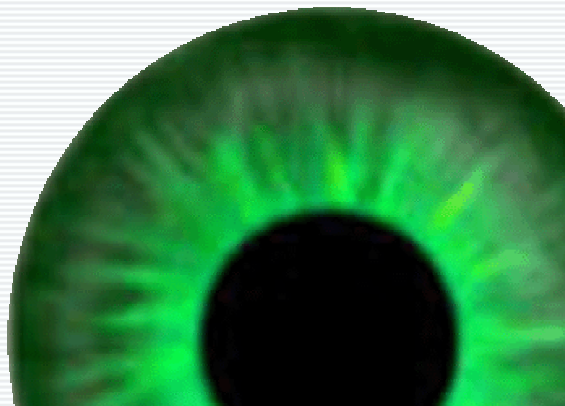
Les attaques psychologiques:

- *Stratégies de dissémination de l'information basées sur la communication virale, la pollination ainsi que le piratage des vecteurs d'information (sites d'information type média, vecteurs d'opinion, Webblogs, mailing list, forums de discussion). Création de la déception par la circulation de rumeurs, publication de communiqués, utilisation des leviers médias, etc…*



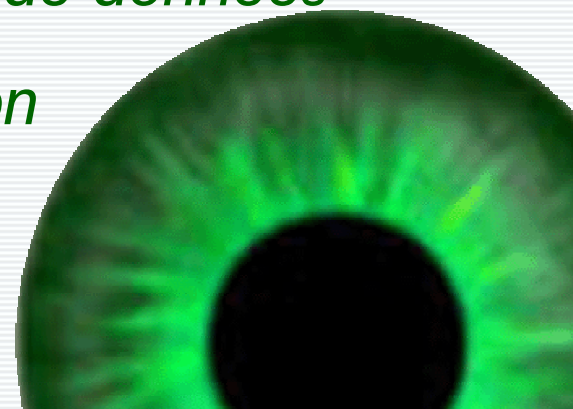
Société de l'information:

Quelques faits survenus dans le passé



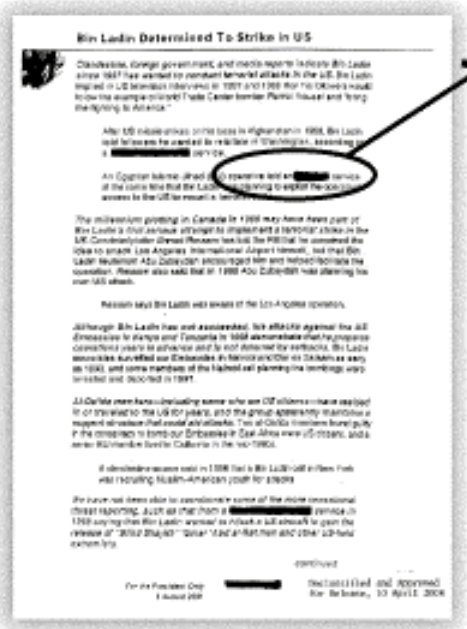
Quelques exemples d'informations sensibles peu protégées

- *Les câbles sous-marin de transport de l'information (fibres optiques: un volume de 10 gigabits seconde, par fibre)*
- *Les plans des infrastructures de transport de l'énergie ou de contrôle à distance du matériel stratégique (équipements hospitaliers, commandes de canalisations)*
- *Tous les « small devices » (print serveur, disque dur de photocopieur et autres supports indirects de données*
- *Les poubelles (augmentation et duplication de la production d'imprimés au sein des entreprises et des administrations)*



QUATRE ÉTAPES POUR DÉVOILER LE MOT MASQUÉ

Le cryptologue David Naccache a retrouvé un mot recouvert à l'encre noire en combinant plusieurs outils informatiques.


Bin Ladin Determined To Strike in US

Déclassifié le 10 avril par la Maison Blanche, le "mémo" adressé le 6 aot 2001 par la CIA à George Bush reste partiellement "caviardé" par souci de protection des sources.

1 Redresser le document

(EIJ) operative told an [redacted] service
adin was planning to exploit the operative's

0,52°

2 Identifier la police de caractère

(EIJ) operative told an [redacted] service
adin was planning to exploit the operative's

→ ARIAL 324

3 Déterminer de la taille du mot

(EIJ) operative told an [redacted] service
adin was planning to exploit the operative's

16 mm

4 Comparer avec le dictionnaire

(EIJ) operative told an [redacted] service
adin was planning to exploit the operative's

→ 1 530 mots candidats

Le mot est précédé par "an",
il commence donc par une voyelle

→ 346 mots candidats

En tenant compte du contexte,
il ne reste plus que...

→ 7 mots candidats

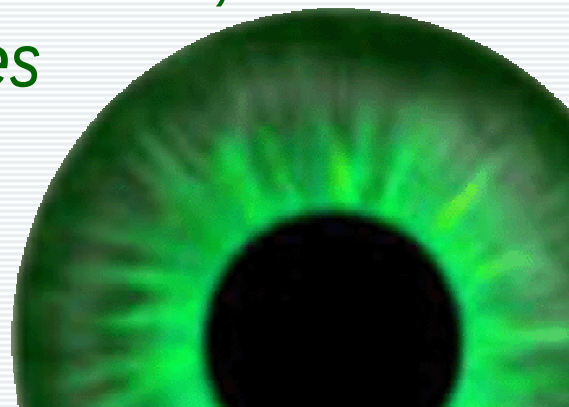
Ukrainian
uninvited
unofficial
incursive
indebted
Ugandan
Egyptian → mot retenu

(EIJ) operative told an Egyptian service
adin was planning to exploit the operative's

LE MONDE | 07.05.04 | 12h58 • MIS A JOUR LE 07.05.04 | 16h13

Concrètement: quelle est la nature du risque?

- *2004: Le programme informatique d'un missile anti-balistique israélien (MOTIF) est contrôlé par un employé égyptiens d'IBM.*
- *2003, 3 morts: un crash logiciel a contribué à une coupure de courant entre les USA et le Canada*
- *2001, 5 morts: Panama, les patients souffrant du cancer meurent les surdosages de radiation, dont les quantités ont été mal déterminées lors de la configuration du logiciel .*

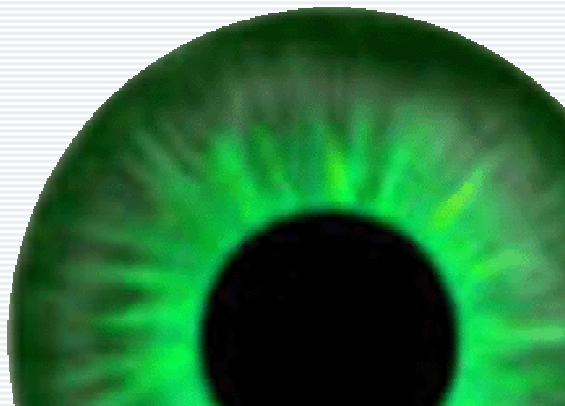


Source: BASELINE MARCH 2004

Intelligentzia.net

Concrètement: quelle est la nature du risque?

- *2000, 4 morts: crash d'un hélicoptère du en partie à un disfonctionnement logiciel*
- *1997, 225 morts: le radar qui aurait été en mesure d'éviter le crash d'un vol de ligne Coréen a eu un disfonctionnement logiciel*
- *1997, 1 mort: une erreur dans le programme d'une seringue automatique a fait injecté une dose mortelle de sulfate de morphine*

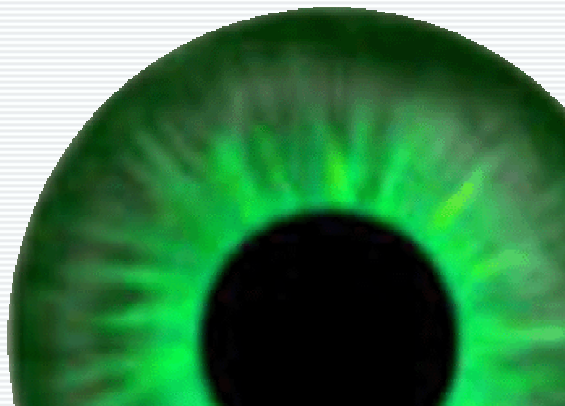


Source: BASELINE MARCH 2004

Concrètement: quelle est la nature du risque?

- *1991, 28 morts: un problème logiciel empêche une batterie de missiles « Patriot » d'intercepter un missile « SCUD » qui touche un baraquement de soldats*

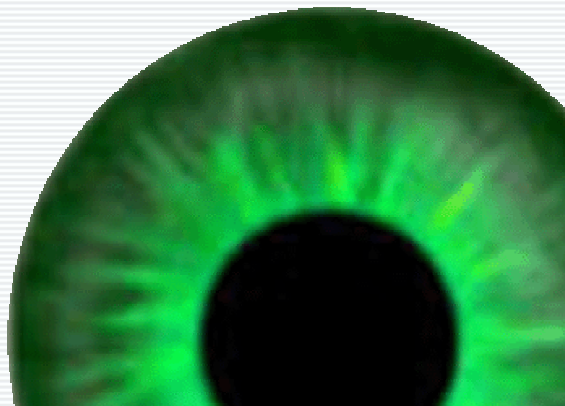
Source: BASELINE MARCH 2004



Le général Uzi Eilam

Ancien responsable des programmes de recherches et de développements militaires en Israël

« La guerre du Golfe nous a montré la nécessité de maîtriser l'ensemble des technologies de l'information pour acquérir le renseignement sur l'ennemi, désinformer l'adversaire, ou orienter l'opinion publique »

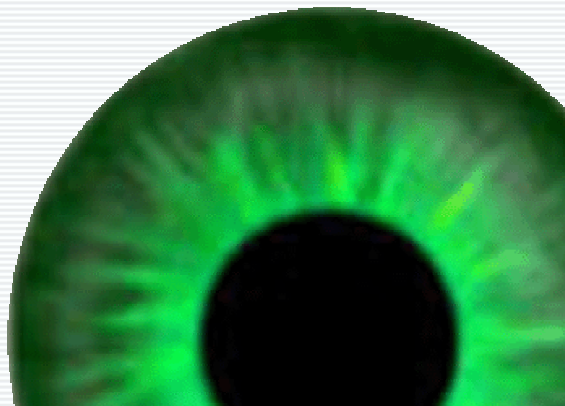


Merci de votre attention ☺

Coordonnées:

Stéphane Koch
www.intelligentzia.net

Mobile: +41 79 607 57 33
Fax: +41 22 731 6007
E-mail: stephane@intelligentzia.net




SYSTEM FAILURE