



MINISTÈRE DE L'ÉCONOMIE  
ET DU COMMERCE EXTÉRIEUR

# Le côté obscur d'Internet

... ou « l'envers du décor »





## **Le côté obscur d'Internet : quelle connaissance?**

**I - L'évidence des menaces numériques**

**II - Un cadre sémantique formalisé**

**III - Types d'actions « *underground* » connues**

**IV - Des statistiques éprouvées**

**V - Des acteurs difficilement « palpables »**

**VI - Quelle prospective pour l'économie numérique?**





## **Le côté obscur d'Internet : quelle connaissance ?**

### **I - L'évidence des menaces numériques**

#### **- Croissance des réseaux d'information et de communication**

-> en corrélation aggravation des **risques** et des **menaces** associés

#### **- Historiquement, Internet n'a pas été développé, dès le départ, de manière sécurisée**

-> supports logiciels et matériels [**vulnérables**]

-> exploitation des failles de sécurité [par **menaces**]

-> danger de pérennité [**impact**]





## Le côté obscur d'Internet : quelle connaissance ?

### I - L'évidence des menaces numériques

#### 1988 : prise de conscience internationale

- > Incident de sécurité peut atteindre tout système informatique
- > Robert **Morris** « lâche » le premier « **ver** » sur Internet
- > A l'époque : **6000 machines** interconnectées **infectées**
- > Déclenche la mise en place des structures de réponse sur incidents en charge de recenser et de traiter ces derniers

(*Computer Emergency & Response Team* – **CERT**)





## Le côté obscur d'Internet : quelle connaissance ?

### I - L'évidence des menaces numériques – [historique]

#### Les années 1980 – Le temps des pionniers

-> Dès 1981, **Ian Murphy** est officiellement la première personne **inculpée** pour un **crime informatique**, aux Etats-Unis

[intrusion dans le système informatique de « AT&T », et modification du programme de facturation, étendant les « heures creuses » à toute la journée...]

-> En 1989, le phénomène des **virus** prend de l'ampleur, on en découvre une trentaine...





## Le côté obscur d'Internet : quelle connaissance ?

### I - L'évidence des menaces numériques – [historique]

#### Les années 1990 – Prise de conscience du phénomène

#### « cybercrime »

-> seconde arrestation de **Kevin Mitnick**, recherché par le FBI pendant 7 ans, pour avoir détourné des informations confidentielles, piraté des centraux téléphoniques et violé des correspondances électroniques (**5 ans de prison**)



-> En 1996, *Concept*, le premier virus macro infectant les documents Word, devient le virus le plus répandu dans le monde



## Le côté obscur d'Internet : quelle connaissance ?

### I - L'évidence des menaces numériques – [historique]

#### Les années 1990 – Prise de conscience du phénomène

#### « cybercrime »

-> En 1998, un groupe de *hackers* dénommé « *The Cult of the Dead Cow* » développe **Back Orifice**, un « cheval de Troie » permettant un accès complet aux ordinateurs infectés

-> En 1999, le virus **Melissa** créé par David Smith entraîne une panique dans le monde et cause plus de « 80 millions de dollars » de dégâts





## Le côté obscur d'Internet : quelle connaissance ?

### I - L'évidence des menaces numériques – [historique]

#### Les années 2000 – Le champ de bataille « Internet »

- > En 2000 : serveurs de sociétés symboles de la « nouvelle économie » font l'objet d'**assauts électroniques concentrés**; des centaines de milliers d'internautes dans le monde reçoivent une déclaration d'amour : « **I Love You** » (virus de type ver)
- > 2004 : 18 millions d'e-mails de type *phishing* ont été interceptés
- > 2006 : sophistication des menaces : *spear phishing*, virus/mobiles, vers/PDA, développement des réseaux de robots (*botnets*), vitalité des chevaux de Troie, et des *malwares*...





## Le côté obscur d'Internet : quelle connaissance ?

### **II – Un cadre sémantique formalisé**

- « *L'émergence de l'ère informatique a donné naissance à de nouveaux comportements délinquants, difficiles à appréhender et marqués du sceau de l'immatérialité* »

-> *La criminalité sur l'Internet* (Pansier, Jez, 2000)

- « *La cyberdélinquance est devenue si commune que désormais la notion fait partie de notre vocabulaire, définie comme un crime commis sur un réseau informatique, particulièrement sur Internet* »

-> *Trends in cybercrime : the dark side of the Internet* 10  
(Hoar, 2005)





## **Le côté obscur d'Internet : quelle connaissance ?**

### **II – Un cadre sémantique formalisé**

**- La notion de « cyberdélinquance » regroupe l'ensemble des infractions commises sur, ou par, un système informatique généralement connecté à un réseau**

**- Deux catégories de menaces principales :**

- 1) Les menaces non intentionnelles, de type accidentelles (pannes, accidents naturels), ou bien fortuites (erreurs humaines)
- 2) Les menaces intentionnelles : passives (ne modifient pas le comportement du système, parfois indétectables), ou bien actives (modification du contenu de l'information)





## Le côté obscur d'Internet : quelle connaissance ?

### II – Un cadre sémantique formalisé

**2006** : *Petit Larousse* -> premières définitions des termes  
« cybercriminalité », « hacker » et « pirate informatique »

-> **Cybercriminalité** : « *Ensemble des infractions pénales commises sur les réseaux de télécommunication, en particulier Internet. On distingue les infractions liées aux technologies (virus, piratage, etc.), celles liées aux contenus (racisme, pédophilie, etc.) et celles facilitées par les réseaux (copies illicites de logiciels ou d'œuvres audiovisuelles, etc...) »*





## Le côté obscur d'Internet : quelle connaissance ?

### **III - Types d'actions « underground » connues**

- *Accès et maintien frauduleux dans un système d'information*
- *Lecture illégale des logiciels, fichiers et données*
- *Altération illégale des données, du fonctionnement du système*
- *Suppression illégale des données*
- *Introduction illégale de programmes pirates*
- *Infraction se rapportant au contenu [pédophilie, ...]*
- *Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes*
- *Etc...*





## Le côté obscur d'Internet : quelle connaissance ?

### III - Types d'actions « *underground* » connues

#### Les grandes familles :

- Virus et vers
- Chevaux de Troie
- *Adwares, spywares* et *rootkits*
- Canulars (le *hoax*)
- Tentatives de fraude (fraude dite « à la nigériane »)





## Le côté obscur d'Internet : quelle connaissance ?

### III - Types d'actions « *underground* » connues

- Attaques Web (*defacing*, déni de service distribué, ...)
- Attaques sur la messagerie (*Spam*, *mass mailing*, *mail bombing*, *phishing*, *pharming*)
- *Botnets* (PC *zombies* suite à une infection virale – estimation de plusieurs millions dans le monde...)
- Le chantage...
- Etc...





## Le côté obscur d'Internet : quelle connaissance ?

### IV - Des statistiques éprouvées [Résultats]

- Explosion » d'Internet & développement du « tout numérique » : les relevés d'incidents se sont constamment multipliés, de manière exponentielle
- Plusieurs **indicateurs** permettent de rendre compte de cette activité et d'en dresser le bilan, souvent en terme d'impacts financiers





## Le côté obscur d'Internet : quelle connaissance ?

### IV - Des statistiques éprouvées [Résultats]

- Dernière étude du **Consumer Reports National Research Center** (cabinet de recherche indépendant américain) présente le coût associé au cybercrime à 7,1 milliards de dollars aux Etats-Unis
- Quatrième étude « **e-crime watch survey** » du CERT-CC, rendue récemment, (échantillon de 671 répondants aux Etats-Unis) estime globalement que les pertes associées à des **actes de criminalité** informatique ont **tendance à augmenter**. Les menaces les plus significatives sont généralement externes à l'entité concernée





## Le côté obscur d'Internet : quelle connaissance ?

### **IV - Des statistiques éprouvées [Résultats]**

- De nombreuses autres études informatives sont aussi disponibles,
- > « **Panorama de la cybercriminalité** » édité chaque année par le Club de la Sécurité de l'Information Français (<http://www.clusif.fr>)
- > Enquête annuelle du **CSI/FBI**
  - 2006 : 52 495 000 dollars pertes  
(fraudes financières : 2 556 900 dollars)
  - 2007 : 66 930 950 dollars pertes  
(fraudes financières : 21 124 750 dollars)
- > Confirmation de **l'appât du gain** comme principal **moteur** d'activité de l'« **underground** »





## Le côté obscur d'Internet : quelle connaissance ?

### IV - Des statistiques éprouvées [Tendances]

- Attaques de plus en plus **sophistiquées** [outils d'infection installé via « *iFrame* » (code de redirection qui permet d'afficher dans une page Web un cadre contenant du code HTML local ou distant)]

-> Attaques sur des **sites à haute fréquentation** dans lesquels les internautes ont généralement confiance

-> Redirige l'utilisateur vers un site pirate choisi, et télécharge du code malveillant. Ce dernier s'exécute suite à l'exploitation de vulnérabilités effectives





## Le côté obscur d'Internet : quelle connaissance ?

### IV - Des statistiques éprouvées [Tendances]

- Généralisation de la technique du « **drive-by-download** » (intervention de l'internaute inutile, le simple fait de visiter une page « préparée » [cherche à exploiter les vulnérabilités de la machine] suffit)
- Si une vulnérabilité est trouvée, un « **trojan downloader** » est alors déposé sur la machine de l'utilisateur
- Le « **trojan downloader** » est chargé de récupérer d'autres *malwares* sur Internet, pour usurper l'identité de l'internaute et détourner des sessions





## Le côté obscur d'Internet : quelle connaissance ?

### IV - Des statistiques éprouvées [Tendances]

- **Livre blanc SOPHOS** « Navigation Web » :

-> Début 2008 : 6000 pages Web infectées par jour, soit une toutes les 14 secondes...

-> 83% des pages Web infectées se trouvent sur des sites « légitimes »

- **Enquête GOOGLE** [2008] :

-> 2,3 millions de pages ont été recensées comme étant infectées par des programmes malveillants...

-> 180 000 sites installent automatiquement des programmes malveillants lors de visites d'internautes...





## Le côté obscur d'Internet : quelle connaissance ?

### IV - Des statistiques éprouvées [Tendances]

- Accroissement du « **spear phishing** »
- Recrudescence des « **botnets** » [ENISA estime à plus de six millions d'ordinateurs « *zombies* »; Symantec indique une augmentation de plus de 50 000 machines par jour]
- Augmentation du marché noir : utilisation de *malwares* est devenu un enjeu économique [**marché** évalué à 63 millions d'Euros
- Etude des universitaires J. Franklin et V. Paxson]
- Augmentation du **blanchiment d'argent**





## Le côté obscur d'Internet : quelle connaissance ?

### IV - Des statistiques éprouvées [Tendances]

- Croissance fulgurante des **menaces** associées au monde virtuel [qui devrait dépasser celles du monde réel selon les prévisions de Mc Afee pour 2008] : développement des sites de paris ou de jeux en ligne, les sites de casinos en ligne, et surtout les sites de banque en ligne [utilisation de *malwares* de type « **password-stealer** » (voleur de mots de passe)]
- Augmentation des attaques VoIP [+50% pour 2008 selon Mc Afee]





## Le côté obscur d'Internet : quelle connaissance ?

### IV - Des statistiques éprouvées [Tendances]

- **Fragilité des sites de réseaux sociaux** [associé au nouveau « terrain de chasse » représenté par Web 2.0]
- **Explosion** attendue du nombre de **virus** [le cap de 1 million de virus devrait être franchi d'ici la fin de 2008, selon F-Secure (rapport de sécurité premier trimestre 2008)]
- Espionnages divers seront aussi en augmentation, facilités par les informations disponibles facilement via les **sites communautaires** [rapport SANS 2008]
- **Le piratage rapporte désormais plus que le trafic de drogue!**





## Le côté obscur d'Internet : quelle connaissance ?

- Les pratiques et technologies de cybercrime sont de plus en plus sophistiquées
  - Les attaques sont de plus en plus nombreuses
  - Les systèmes d'information et de communication sont exposés et potentiellement vulnérables
  - Le nombre d'incidents de sécurité progresses
  - Le vol d'informations [personnelles, confidentielles] et l'appât du gain : **nouvelles convoitises**
- > **Le cybercrime devient réellement « organisé »...**





## Le côté obscur d'Internet : quelle connaissance ?

### V – Des acteurs difficilement « palpables »

- a - Le reflet médiatique dominant du pirate informatique
- b - Le point de vue des acteurs
- c - Le point de vue des experts





## Le côté obscur d'Internet : quelle connaissance ?

### V – Des acteurs difficilement « palpables »

- Cybercrime socialement construit, *via* notamment la médiatisation d'un **état technique et statistique conséquent**
- Au-delà des attaques techniques connues, **quid de l'être humain** à l'origine des attaques?
- Le « hors-la-loi » numérique ou « pirate informatique » : élément principal **déclencheur du risque numérique**, et véritable **origine du danger** sur les réseaux informatiques
- Ce dernier reste cependant **difficilement « palpable »** en terme de connaissance





## Le côté obscur d'Internet : quelle connaissance ?

- Image de cet agent menaçant non maîtrisée par l'opinion publique :

- **absence de mise en relation directe,**
- **ignorance de ce contexte social**

- Citoyen ne peut finalement que **se représenter** le « hors-la-loi » numérique, ou à l'inverse, tout simplement **ignorer** cet acteur « dangereux »

- L'agent menaçant demeure véritablement à un niveau d'accès et de compréhension très **opaque**, justifiant le terme « underground » (mouvement clandestin)





## Le côté obscur d'Internet : quelle connaissance ?

- Quant à la représentation de l'acteur menaçant, plusieurs mondes sociaux y participent :

-> **les médias** (principal vecteur d'information quant à la cyberdélinquance)

-> **les experts de la sécurité de l'information**

-> **le monde « *underground* »**

Trois « mondes de la cyberdélinquance », comme spécifiquement attachés à la construction et à la diffusion des significations sociales relatives au pirate informatique





## **Le côté obscur d'Internet : des acteurs difficilement « palpables »**

### **a - Le reflet médiatique dominant du pirate informatique**

- Représentations médiatiques du pirate informatique : nombreuses *via* différents médias (cinéma, presse écrite, télévision, Internet...)
- Effet de cadrage des médias conduit à la construction d'un

### **univers mental de représentations**

- > une image plus ou moins positive et une acceptabilité sociale plus ou moins étendue d'une activité donnée





## **Le côté obscur d'Internet : des acteurs difficilement « palpables »**

### **a - Le reflet médiatique dominant du pirate informatique**

- Discours médiatiques -> deux grandes tendances :

#### **1 - Volonté d'informer et d'instruire sur ce phénomène**

-> but d'éveiller les consciences face à une menace afin  
de susciter chez les utilisateurs la nécessité de se doter de  
systèmes d'information sécurisés

-> montrer le caractère illégal du cybercrime





## Le côté obscur d'Internet : des acteurs difficilement « palpables »

### a - Le reflet médiatique dominant du pirate informatique

- Discours médiatiques -> deux grandes tendances :

**2** - Approfondissement de la connaissance sur le sujet à travers une réflexion sur le profil type du « **hacker** », et de sa philosophie, ainsi que de la culture « **underground** »





## Le côté obscur d'Internet : des acteurs difficilement « palpables »

### a - Le reflet médiatique dominant du pirate informatique

- Les médias ont tenté de déterminer la différence entre les  
« *hackers* » et les « *crackers* »

-> L'image des « *hackers* » se voit souvent mise en valeur :  
définition de passionnés qui aiment les défis et maîtrisent à la  
perfection les moindres détails des systèmes d'information et de  
communication





## **Le côté obscur d'Internet : des acteurs difficilement « palpables »**

### **a - Le reflet médiatique dominant du pirate informatique**

- Danger du besoin de convaincre [risque d'occulter le besoin de véracité]
- > image du « héros », du génie à la recherche du challenge, pour des faits qualifiés comme illégaux [souvent de gravité extrême]
- > danger des communications facilitant le « marketing de la peur »
- > ce mélange des genres : peut troubler la compréhension





## **Le côté obscur d'Internet : des acteurs difficilement « palpables »**

### **a - Le reflet médiatique dominant du pirate informatique**

-> Clivages du discours : difficulté de représentations  
par l'utilisateur des TICs, voire l'erreur de représentation  
« citoyenne »

-> Un amalgame dangereux entre des **faits illégaux** et des  
**acteurs sociaux exclus de toute responsabilité**, devient  
alors possible au sein des représentations sociales





## Le côté obscur d'Internet : des acteurs difficilement « palpables »

### b - Le point de vue des acteurs

- Monde « *underground* » regroupe
  - > **pirates informatiques** (“*crackers*”, “*black hat*”...)
  - > monde du « **hacking** » (“*hackers*”, “*white hat*”...)
- Monde très difficile à percevoir, dénomination  
« **underground** » détermine toute l’opacité de ce milieu





## **Le côté obscur d'Internet : des acteurs difficilement « palpables »**

### **b - Le point de vue des acteurs**

#### **- Hacking :**

-> volonté de faire connaître et reconnaître ses talents

-> recherche d'un challenge informatique

-> transfert des connaissances

-> reconnaissance par les pairs

-> ...





## Le côté obscur d'Internet : des acteurs difficilement « palpables »

### b - Le point de vue des acteurs

#### - Hacking :

- > lutte pour la diffusion d'une image positive
- > refuse toute labellisation comme criminel

- Lutte ne semble pas vaine, dichotomie souhaitée « Hackers / Crackers » apparaît dans divers écrits journalistiques ou grand public, mais aussi au sein du monde des experts de la sécurité de l'information





## Le côté obscur d'Internet : des acteurs difficilement « palpables »

### b - Le point de vue des acteurs

- Au sein de l' « **underground** », cela n'occulte pas la réalité des « hors-la-loi » du numérique qui peuvent entraîner de graves impacts de nature diverse
- D'autre part, malgré toute bonne volonté affichée, en rapport à toute attaque informatique, la loi est claire : ce type d'acte demeure dans tous les cas répréhensible





## Le côté obscur d'Internet : des acteurs difficilement « palpables »

### c - Le point de vue des experts

- Professionnels spécialisés en sécurité technique et/ou organisationnelle de l'information :

-> développant des offres de **produits** et de **services** adaptés

-> sont à l'origine de nombreuses **bases de connaissances** de

**menaces ciblées** permettant, par exemple, de prendre conscience des profils possibles des attaquants





## Le côté obscur d'Internet : des acteurs difficilement « palpables »

### c - Le point de vue des experts

- Au cœur du risque de sécurité, les experts estiment que la menace, de type acteur humain malveillant :

-> constitue l'**élément le plus difficile à cerner**

-> surtout du point de vue de son identification sociale

et de son niveau de dangerosité





## Le côté obscur d'Internet : des acteurs difficilement « palpables »

### c - Le point de vue des experts

- Pour en faciliter l'approche compréhensive, la structure **CASES** (**Cyberworld Awareness & Security Enhancement Structure** – <http://www.cases.public.lu>), portail national luxembourgeois de la sécurité de l'information :

-> a notamment structuré l'approche des trois profils catégorisés des cyberdélinquants [**hackers, crackers, script kiddies**], en rédigeant deux fiches didactiques de l'objet social « cyberdélinquance »





## Le côté obscur d'Internet : quelle connaissance ?

### VI – Prospective pour l'économie numérique

- Entreprises européennes : **20% des investissements** pour les Technologies de l'Information et de la Communication (TICs)
- Secteur TICs : **26%** de la totalité des **dépenses de recherche européennes**
- **60% des services publics** sont disponibles en ligne [UE]
- + **50% des citoyens** de l'UE **utilisent Internet** régulièrement
- ...
- > **Le dynamisme des TICs joue un rôle grandissant pour la croissance économique (1/4 de la croissance mondiale)**





## **Le côté obscur d'Internet : quelle connaissance ?**

### **VI – Prospective pour l'économie numérique**

- a – Les solutions existantes
- b – Le concept de « confiance numérique »
- c – ILNAS & « confiance numérique »





## Le côté obscur d'Internet : prospective & économie numérique

### a - Les solutions existantes [Face aux menaces]

- Nécessaire sensibilisation au phénomène et aux moyens de protection
- Nécessaires informations et communication [adaptées]
- Lutte contre la cybercriminalité
- Importance de la coopération internationale
- Maîtrise de la connaissance des TICs
- Etc...





## Le côté obscur d'Internet : prospective & économie numérique

### **b – Le concept de « confiance numérique »**

#### **La confiance numérique :**

- adopter des technologies de sécurité de pointe,
- mais surtout prouver que les technologies et pratiques utilisées sont fiables
- user de communication ouverte et de transparence



- > une stratégie d'entreprise qui vise l'excellence
- > conserver l'implication constante des clients, des partenaires, et des citoyens



## Le côté obscur d'Internet : prospective & économie numérique

### c – ILNAS & « confiance numérique »

#### La « confiance numérique » :

-> un des services de l'administration **ILNAS** [Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services]





## Le côté obscur d'Internet : prospective & économie numérique

### c – ILNAS & « confiance numérique »

**ILNAS** intègre [principalement] :

- OLAS [Office Luxembourgeois d'Accréditation et de Surveillance]
- Organisme Luxembourgeois de Normalisation
- La métrologie légale
- La surveillance du marché
- La sécurité générale des produits
- La promotion du management de la qualité...
- Toute autre mission qui lui sera assignée par le Gouvernement





## Le côté obscur d'Internet : prospective & économie numérique

### c – ILNAS & « confiance numérique »

#### Service « Confiance Numérique »/ILNAS :

- > travail de **prospective du domaine** comme support essentiel pour servir une économie nationale à la fois efficace et compétitive
- > **relais d'informations** vers les entités nationales concernées
- > **suivi des évolutions normatives** du champ de la « confiance numérique »
- > **travail collaboratif** constant avec la structure **CASES**





## Le côté obscur d'Internet : prospective & économie numérique

### c – ILNAS & « confiance numérique »

#### **Service « Confiance Numérique »/ILNAS : [Missions]**

- > **Etudes et développement TICs** [Services ILNAS]
- > Accréditation, notification et surveillance des Prestataires de Services de Certification [selon la *loi modifiée du 14 août 2000 relative au commerce électronique*]
- > Prospective générale du champ : **ISO/IEC/JTC1**  
[« *Joint Technical Committee 1* » - **JTC1** : organe de référence pour la normalisation des TICs au niveau mondial]





## Le côté obscur d'Internet : prospective & économie numérique

### c – ILNAS & « confiance numérique »

#### **Service « Confiance Numérique » /ILNAS : [Missions]**

- Suivi spécifique du sous-comité **JTC1/SC27** (série « 2700x » et groupes *ad hoc...*)
- Promotion et veille des **instruments** garantissant la confiance numérique [certifications ISO/IEC 27001, ISO/IEC 15408, ...]
- **Etudes de projets nationaux** relatifs au développement de la confiance numérique [schémas d'accréditation et/ou de certification]
- **Collaboration** active avec la structure **CASES** [sécurité et confiance TICs]





## Le côté obscur d'Internet – [Outputs]

- Des dangers sont réels
- Des compétences et des solutions techniques existent
- Nécessité de se tenir informé [domaine sécurité]
- Développer une approche « critique » et « objective »
- « *Ne pas noircir le tableau* » [sans raison]
- Profiter « pleinement » de l'économie numérique [mais en connaissance de cause]
- Privilégier les marqueurs de la confiance [si possible]
- ...et en restant attentifs à leur développement...





**Merci pour votre attention**

**jean-philippe.humbert@olas.etat.lu**

**\*\*\***

**\***

**« Les mondes de la cyberdélinquance et  
images sociales du pirate informatique »**



[[http://www.cases.public.lu/fr/publications/recherche/these\\_jph/Memoire\\_PHD\\_JP\\_Humbert.pdf](http://www.cases.public.lu/fr/publications/recherche/these_jph/Memoire_PHD_JP_Humbert.pdf)]