

**Non classifié**

**DSTI/ICCP/IIS(2005)1/FINAL**



Organisation de Coopération et de Développement Economiques  
Organisation for Economic Co-operation and Development

**02-Dec-2005**

**Français - Or. Anglais**

**DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE  
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE  
ET DES COMMUNICATIONS**

**Groupe de travail sur les indicateurs pour la société de l'information**

**ÉTUDE EXPLORATOIRE POUR LA MESURE DE LA CONFIANCE DANS L'ENVIRONNEMENT  
EN LIGNE**

**JT00195478  
TA 72698**

Document complet disponible sur OLIS dans son format d'origine  
Complete document available on OLIS in its original format

**DSTI/ICCP/IIS(2005)1/FINAL  
Non classifié**

**Français - Or. Anglais**

## AVANT-PROPOS

Le présent rapport a été présenté au Groupe de travail sur les indicateurs pour la société de l'information (GTISI) en avril 2005 et au Groupe de travail sur la sécurité de l'information et la vie privée (GTSIVP) en mai 2005. Le Comité de la politique de l'information, de l'informatique et des communications (PIIC) a recommandé de le mettre en diffusion générale en octobre 2005.

Ce rapport a été préparé par Sam Paltridge, Sheridan Roberts et Brigitte van Beuzekom de la Division des analyses économiques et des statistiques de la Direction de la Science, de la Technologie et de l'Industrie. Les auteurs remercient leurs collègues de la Division PIIC, ainsi que les délégués du Groupe de travail sur les indicateurs pour la société de l'information et ceux du Groupe de travail sur la sécurité de l'information et la vie privée, de leur contribution à ce travail.

Le rapport est publié sous la responsabilité du Secrétaire général de l'OCDE.

Copyright OCDE, 2005.

Les demandes d'autorisation de reproduction ou de traduction totale ou partielle de cette publication doivent être adressées aux Éditions de l'OCDE, 2 rue André-Pascal, 75775 Paris Cedex 16, France.

## TABLE DES MATIÈRES

AVANT-PROPOS .....	2
INTRODUCTION .....	5
PARTIE 1 : STATISTIQUES OFFICIELLES SUR LA CONFIANCE DANS L'ENVIRONNEMENT EN LIGNE .....	9
Introduction .....	9
Sécurité informatique .....	9
Autres problèmes de confiance.....	9
Statistiques officielles sur la confiance .....	9
Enquêtes sur l'utilisation des TIC par les entreprises.....	9
Enquêtes spécialisées sur la sécurité des technologies de l'information .....	11
Enquêtes sur l'utilisation des TIC auprès des ménages .....	11
Exemples de données officielles.....	12
Évolutions futures : les enquêtes types de l'OCDE sur l'utilisation des TIC par les entreprises et les ménages.....	12
Enquête type auprès des entreprises .....	12
Enquête type auprès des ménages.....	13
PARTIE 2 : STATISTIQUES SUR LA CONFIANCE DANS L'ENVIRONNEMENT EN LIGNE ÉMANANT DE SOURCES SEMI-OFFICIELLES ET PRIVÉES.....	14
Enquêtes sur les perceptions, les opinions et les usages .....	14
L'enquête de la Direction GOV de l'OCDE sur l'administration électronique.....	14
L'eurobaromètre de la Commission européenne .....	15
Enquêtes par l'industrie .....	16
Enquêtes de l'industrie sur les usages d'Internet.....	17
Le Pew Internet & American Life Project.....	18
Consumer Reports .....	18
Enquêtes réalisées par des professionnels de la sécurité et des organismes chargés de l'application des lois .....	18
Statistiques sur les plaintes des consommateurs et les fraudes sur Internet .....	22
Consumer Sentinel.....	22
Internet Fraud Complaint Center .....	22
National Fraud Information Center et Internet Fraud Watch .....	23
Econsumer.gov .....	23
Ventes de détail, sécurité et fraude en ligne.....	23
Statistiques sur la criminalité .....	24
Criminalité liée au vol d'identité et cybercriminalité.....	25
Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et autres initiatives des pays européens en matière de sécurité .....	26
Exemples choisis de menaces/attaques/incidents sur Internet et disponibilité des données .....	26
Hameçonnage et « pharming » .....	26
Logiciels espions .....	30
Virus, vers, chevaux de Troie et autres incidents .....	32

Botnets (machines zombies).....	34
Prise de contrôle du modem .....	37
Fraude par clic et « référencement abusif ».....	38
Sécurité et certification de l'infrastructure de commerce électronique.....	39
Secure socket layer (SSL).....	39
ANNEXE 1 : QUELQUES STATISTIQUES OFFICIELLES SUR LA CONFIANCE (VIS-À-VIS DE L'ENVIRONNEMENT CONNECTÉ) .....	43
Eurostat .....	43
Données des entreprises sur la sécurité informatique.....	43
Données des ménages sur la sécurité informatique .....	44
Australie.....	45
Canada.....	46
Japon .....	47
États-Unis.....	47
ANNEXE 2 : PROJET DE QUESTIONS OCDE TYPES SUR LA CONFIANCE .....	48
Projet de questionnaire OCDE type concernant l'utilisation des TIC par les entreprises (arrêté à avril 2005).....	48
Section A : informations générales sur l'utilisation des TIC par votre entreprise.....	48
Section B : sécurité informatique .....	49
Section C : comment votre entreprise utilise-t-elle les TIC dans son fonctionnement ?.....	50
Questionnaire OCDE type révisé concernant l'utilisation des TIC par les ménages et les particuliers (arrêté à août 2005) .....	51
Section A : accès des ménages aux technologies de l'information et des communications.....	51
Section B : Utilisation des technologies de l'information et des communications par les individus (adultes).....	52
ANNEXE 3 : QUELQUES STATISTIQUES SUR LA CONFIANCE ISSUES DE SOURCES PRIVÉES ET SEMI-OFFICIELLES .....	55
NOTES .....	71

## INTRODUCTION

Un élément fondamental pour concrétiser les retombées que l'on peut attendre des technologies de l'information et des communications (TIC) en matière de développement socio-économique est la confiance que les utilisateurs accordent aux plates-formes, applications et services. La création d'un environnement en ligne renforçant la confiance parmi les utilisateurs des réseaux d'information et de communication est une priorité croissante pour les entreprises, l'industrie et les pouvoirs publics, et c'est l'un des thèmes à l'ordre du jour de l'OCDE depuis la fin des années 1990.<sup>1</sup> L'objet du présent rapport est donc de passer en revue les données disponibles auprès de sources officielles, semi-officielles et privées susceptibles de contribuer à éclairer les évolutions et progrès dans ce domaine. Il faut en effet être en mesure d'exploiter les données pertinentes pour évaluer l'efficacité des initiatives publiques et privées destinées à renforcer la confiance parmi les utilisateurs. Cela revêt d'autant plus d'importance que l'accès à Internet, de même que son usage, continuent de croître dans l'ensemble de la zone de l'OCDE.

Fin 2003, on dénombrait 260 millions d'abonnés à Internet disposant d'un accès fixe — alors que le chiffre n'était que d'un peu plus de 100 millions en 1999.<sup>2</sup> Etant donné que chacun de ces comptes est utilisé par plusieurs personnes, dans les foyers ou les entreprises, le nombre des personnes qui accèdent à Internet est naturellement beaucoup plus élevé. Fin 2003, près d'un tiers de l'ensemble des abonnés disposaient d'un accès haut débit à Internet, permettant des connexions beaucoup plus rapides et permanentes. Ce taux devrait progresser rapidement dans les prochaines années. Par ailleurs, les premières plates-formes à haut débit permettant un accès par réseau sans fil cellulaire ont été introduites, et devraient contribuer à accroître encore l'accès et l'utilisation d'Internet.

Avec le développement des réseaux, les nouvelles possibilités offertes multiplient les opportunités mais aussi les enjeux. Le fait que la connexion à haut débit soit permanente, par exemple, renforce le besoin pour les particuliers et les petites entreprises de se protéger au moyen d'outils tels que pare-feux, autrefois l'apanage exclusif des réseaux d'entreprise. De plus, avec les performances accrues du haut débit, les systèmes piratés sont davantage susceptibles de nuire à d'autres systèmes. C'est notamment le cas avec l'émergence de ce que l'on appelle les « botnets » ou réseaux de robots. Cette expression désigne un groupe de machines piratées (« zombies »), agissant de concert, à l'insu de leurs propriétaires, utilisées pour attaquer d'autres utilisateurs ou retransmettre du spam. Il existe toute une foule d'autres menaces, notamment le hameçonnage (« phishing »), les logiciels espions (« spyware »), les virus et différentes formes d'usurpation d'identité et de prise de contrôle de pages Web. En revanche, les connexions haut débit permettent à l'industrie des TIC de fournir des technologies continuellement actualisées et améliorées, directement aux utilisateurs, de manière à prévenir l'endommagement et l'utilisation abusive de leurs systèmes. Les mises à jour de technologies de protection comme les pare-feu et logiciels anti-virus, qui sont facilitées par les connexions permanentes, en sont un exemple.

Les gouvernements des pays de l'OCDE sont convenus d'un certain nombre d'initiatives visant à forger une culture de confiance et de sécurité. Au niveau international, on peut notamment mentionner les *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information*, les *Orientations politiques et pratiques de l'OCDE concernant la protection de la vie privée en ligne* et les *Lignes directrices de l'OCDE régissant la protection des consommateurs dans le contexte du commerce électronique*. Le secteur privé a également été actif. De nombreuses initiatives ont été lancées, depuis les partenariats tels que l'*Anti-Phishing Working Group*, jusqu'à la mise en oeuvre d'outils visant à renforcer

la confiance directement auprès des utilisateurs, comme les chartes de protection de la vie privée, les marques de confiance et les serveurs sécurisés.

Le présent document passe en revue les sources statistiques disponibles qui sont susceptibles d'apporter des éclairages sur ces questions, et il vise à contribuer à la poursuite de l'élaboration de statistiques utiles. Sur ce dernier point, il importe de garder à l'esprit qu'il existera toujours des limitations pratiques quant au nombre et à la nature des indicateurs pouvant être recueillis par les organismes statistiques officiels. Le thème des TIC suscite de nombreuses demandes d'informations dans un vaste ensemble de domaines. La confiance, bien que très importante, est en concurrence avec d'autres domaines majeurs nécessitant des informations concernant les TIC.

Jusqu'à présent, la principale démarche des organismes statistiques officiels a consisté à recueillir des données au moyen d'enquêtes auprès des ménages et des entreprises sur l'utilisation des TIC. A cette occasion, des informations sur la confiance sont fréquemment recueillies, par exemple par le biais de questions spécifiques sur la sécurité des TI ou sur les éléments touchant la confiance perçus comme des obstacles à l'utilisation d'Internet ou au commerce sur Internet. La valeur de cette information tient aux points forts traditionnels des bureaux statistiques nationaux, notamment à la transparence et à la définition précise des méthodologies, à l'intégration des cadres conceptuels, à la vaste taille des échantillons et au taux relativement élevé de réponses.

Un ensemble d'autres organismes gouvernementaux recueillent également des données utiles pour éclairer les questions liées à la confiance et à la sécurité. C'est notamment le cas des organismes chargés de l'application des lois et de la protection des consommateurs. Ces données sont recueillies dans le cadre des procédures traditionnelles que mettent en œuvre ces organismes, dans les enquêtes qu'ils réalisent et en liaison avec d'autres mécanismes qu'ils ont créés pour permettre aux entreprises et aux consommateurs de signaler les incidents. La mesure de la cybercriminalité est un domaine d'activité qui se développe, notamment la criminalité liée au vol d'identité.

La publication de données mesurant la sécurité des systèmes et réseaux d'information exploités par les pouvoirs publics, bien que limitée, se développe. Le *Federal Information Security Management Act* (FISMA), de 2002, impose des évaluations de sécurité et un cycle continu d'évaluation des risques dans tous les organismes fédéraux aux Etats-Unis.<sup>3</sup> Le *General Accounting Office* (GAO) des États-Unis publie régulièrement des rapports sur la mise en œuvre de ce texte et publie des données à ce sujet.<sup>4</sup> Au Canada, dans le cadre de la politique du gouvernement sur la sécurité (PGS), les services fédéraux sont tenus de mener une politique active de surveillance et d'audit interne de leurs programmes de sécurité et de rendre compte des résultats au Secrétariat du Conseil du Trésor du Canada. Aux Pays-Bas, le ministère des Affaires économiques publie un certain nombre d'études de référence quantitatives et qualitatives de caractère plus général concernant les tendances dans le secteur des TIC, notamment en matière de sécurité des réseaux (par exemple *Netwerken in cijfers* (TNO) et *Digital Economy* (Statistiques Pays-Bas)). De plus, le TNO a publié en mars 2005 une étude demandée par le ministère des Affaires économiques destinée à trouver des indicateurs susceptibles d'aider le ministère dans sa tâche d'élaboration des politiques dans le domaine de la sécurité des réseaux. En Finlande, le ministère des Finances publie un bilan annuel de l'utilisation des TIC au sein du gouvernement comprenant un ensemble d'indicateurs sur la sécurité des réseaux et des services dans ses diverses agences.

Le secteur privé est souvent mieux placé pour produire des données capables d'éclairer les questions de confiance et de sécurité en ce qui concerne les entreprises et autres utilisateurs. On peut également classer dans ce groupe les organismes à but non lucratif qui reçoivent des fonds publics et s'occupent de sécurité sur Internet. En effet, de par sa nature même, l'Internet permet de communiquer des données sur les incidents directement aux fournisseurs d'outils tels que pare-feu et logiciels anti-virus. L'un des points forts de ces données est qu'elles sont générées automatiquement et peuvent être mises en temps réel à la

disposition des utilisateurs de ces produits, par l'intermédiaire des sites Web des éditeurs. En revanche, l'information recueillie peut, dans certains cas, ne traduire la situation que des clients d'une société donnée. Cela peut donc ne permettre de tirer de ces données que des conclusions limitées par rapport à l'ensemble du marché. Les technologies utilisant des navigateurs Web pour l'échange entre utilisateurs d'informations sur les menaces, sites Web frauduleux par exemple, peuvent également produire des informations en temps réel sur les tendances dans le domaine de la sécurité.

Les entreprises du secteur privé et les organismes publics agissent également à travers la création d'associations qui parrainent le recueil ou le regroupement de statistiques dans leurs propres domaines d'activité. On peut citer notamment l'*Anti-Phishing Working Group* aux États-Unis et l'*Association for Payment and Clearing Services (APACS)* au Royaume-Uni.

Le présent rapport comprend deux parties. La première est consacrée aux statistiques officielles et l'autre aux sources privées et semi-officielles. L'annexe donne des exemples de données disponibles et des références à d'autres sources. Pour l'avenir, les travaux de l'OCDE sur la mesure de la confiance dans l'environnement en ligne pourraient s'organiser selon plusieurs axes. L'un consisterait à continuer de réviser périodiquement dans les enquêtes types de l'OCDE les questions sur l'utilisation des TIC par les entreprises et les ménages, dont les plus récentes révisions proposées sont reproduites dans le présent rapport, et d'encourager leur adoption par les pays membres dans leurs propres enquêtes. Pour de nombreux pays, il subsisterait néanmoins une lacune importante, pour l'évaluation des questions qui entourent la confiance, concernant l'utilisation en ligne et l'offre de services gouvernementaux, dans le secteur public.

L'enquête sur l'administration électronique conduite par la Direction de la gouvernance publique et du développement territorial de l'OCDE (GOV) est une autre source possible d'informations, mais elle est limitée aux pays faisant l'objet d'un examen par les pairs et à l'année pour laquelle ces études sont réalisées. Une autre limitation est que les questions qui entourent la confiance, bien qu'incontestablement d'une grande importance, sont en concurrence avec d'autres domaines qui intéressent fortement les pouvoirs publics dans ces enquêtes. Une solution possible de remplacement serait une enquête type de l'offre et de l'utilisation des TIC axée sur le secteur public. Il faudrait toutefois que les décideurs identifient les aspects de la confiance qu'ils considèrent comme les plus importants à mesurer dans le secteur public, que soit élaborée une enquête type et qu'un ou plusieurs pays se portent volontaires pour tester les questions. Il faut noter que les bureaux nationaux de statistiques ont fait état de difficultés dans la collecte d'informations concernant les TIC auprès d'organisations gouvernementales. Les principales difficultés sont la définition des unités administratives et l'hétérogénéité de ces unités, par exemple, les différences dans la façon dont les fonctions en matière de TIC sont organisées et les évolutions des structures organisationnelles au fil du temps. Ces facteurs font qu'il est très difficile de procéder à une comparaison valide des données entre régions, niveaux d'administration et périodes.

Peu de pays de l'OCDE procèdent actuellement à des mesures sur les questions qui entourent la confiance en ce qui concerne le secteur public. Le Canada fait toutefois exception en exigeant que figure une charte de protection de la vie privée sur les sites Web institutionnels et en publiant des données séparées pour les secteurs public et privé. La Hongrie est un autre exemple. Depuis 2003, le Bureau central de statistiques hongrois a étoffé son enquête auprès des administrations publiques (administrations d'État et municipalités) pour y inclure des questions sur l'utilisation des TIC, la sécurité informatique, le nombre de services publics en ligne avec procédures d'arrière-guichet intégrées et les procédures de marchés publics qui sont entièrement réalisées en ligne. L'enquête hongroise comporte également des questions sur les ordinateurs (nombre, âge, valeur), la formation aux TIC et l'investissement dans les TIC dans le secteur public.

L'une des conclusions qui peut être tirée des données réunies dans le présent rapport est que les coûts économiques directs des phénomènes liés à la confiance, tels que la sécurité et la vie privée, augmentent rapidement. Les éléments disponibles pointent tous vers une forte progression de la cybercriminalité, comme le vol d'identité ou la fraude en ligne, intrinsèquement liée au développement de l'utilisation des TIC. Les publications sur les aspects économiques de la confiance sont relativement récentes mais constituent un domaine qui se développe et qui bénéficierait de travaux auxquels participeraient des pays membres.<sup>5</sup> De plus, une bonne partie des données statistiques qui sont disponibles auprès de sources non officielles sur, par exemple, le coût économique des incidents (par exemple attaques par virus ou déni de services) ne s'accompagnent pas de données transparentes et bien documentées sur les méthodologies utilisées. Néanmoins, elles sont fréquemment le signe avant-coureur d'estimations nationales et internationales plus vastes utilisées pour solliciter des ressources publiques et privées.

Une première étape dans l'amélioration de la disponibilité des données serait de rechercher un accord international sur des définitions de concepts comme la cybercriminalité ou la sécurité, pour lesquels des travaux sont déjà en cours dans certains organismes statistiques officiels. On pourrait imaginer d'organiser dans quelque temps à l'OCDE un séminaire ou une réunion de groupe d'experts sur la mesure de la confiance. Ce séminaire pourrait réunir des représentants des organismes statistiques officiels ainsi que d'autres institutions, par exemple services chargés du contrôle de l'application des lois et de la protection des consommateurs et organismes du secteur privé, travaillant dans ce domaine. L'un des buts de ce séminaire pourrait être de s'appuyer sur l'expérience acquise et de développer des définitions reconnues au plan international des concepts liés à la confiance dans l'environnement en ligne.

## **PARTIE 1 : STATISTIQUES OFFICIELLES SUR LA CONFIANCE DANS L'ENVIRONNEMENT EN LIGNE**

### **Introduction**

Le thème de la confiance dans l'environnement en ligne est vaste, et il recouvre notamment la sécurité informatique, la vie privée et des questions telles que la protection des consommateurs. Pour mesurer cette confiance, on peut considérer chacun de ces trois sous-thèmes. Toutefois, en pratique, la plupart des travaux dans les statistiques officielles ont porté sur le domaine de la sécurité informatique, certaines données étant également recueillies sur les problèmes liés à la protection de la vie privée et de la confiance.

### *Sécurité informatique*

La sécurité informatique est un défi tant pour les internautes que pour ceux qui mesurent l'utilisation des TIC. Dans les statistiques officielles, elle est généralement considérée comme une question de mesure du côté de la demande, et des questions peuvent être ajoutées dans les enquêtes sur l'utilisation des TIC par les ménages et les entreprises réalisées dans de nombreux pays de l'OCDE. Pour les entreprises, la méthode habituelle de mesure consiste à inclure des questions dans une enquête sur l'utilisation des TIC par les entreprises ou à procéder à une enquête distincte sur la sécurité des TIC ciblée sur les entreprises. Pour les ménages, des questions sont en général ajoutées dans les enquêtes sur l'utilisation des TIC par cette catégorie d'utilisateurs.

Les questions sur la sécurité des TI abordent en général les problèmes de sécurité rencontrés par les déclarants, l'origine ou les conséquences de ces problèmes et les mesures de prévention mises en place. Pour les entreprises, des questions peuvent également porter sur les coûts financiers. Par ailleurs, dans les enquêtes auprès des ménages comme des entreprises, la sécurité informatique est souvent mentionnée comme une réponse possible aux questions sur les obstacles au commerce électronique et à l'accès à Internet.

### *Autres problèmes de confiance*

Les questions liées à la confiance qui sortent du cadre de la sécurité informatique sont moins souvent traitées dans les statistiques officielles. Toutefois, on dispose de certaines données sur les pratiques de renforcement de la confiance par les entreprises dans les pays qui procèdent à l'Enquête communautaire d'Eurostat sur l'utilisation des TIC et du commerce électronique dans les entreprises, et grâce à Statistique Canada avec son Enquête sur le commerce électronique et la technologie. Il existe également des données émanant d'un certain nombre de pays sur les problèmes de vie privée et de confiance en tant qu'obstacle au commerce électronique et à l'accès à Internet. Les questionnaires auprès des ménages peuvent comporter des rubriques sur les problèmes de vie privée ou d'accès des enfants à Internet.

### **Statistiques officielles sur la confiance**

#### *Enquêtes sur l'utilisation des TIC par les entreprises*

Plusieurs pays, notamment l'Australie, le Canada, le Japon et les pays appartenant à la Commission européenne (via le questionnaire type d'Eurostat) procèdent à ce type d'enquête.

Les questionnaires d'Eurostat pour 2004 et 2005 comportent un certain nombre de questions sur la sécurité informatique et sur d'autres thèmes en relation avec la confiance, à savoir :

- Les moyens de sécurité interne en place.
- L'utilisation de communications sécurisées par signature électronique, etc.
- Les mises à jour des moyens de sécurité au cours des trois derniers mois.
- Les problèmes de sécurité informatique rencontrés au cours des douze derniers mois et, en cas de réponse positive, la nature de ces problèmes.
- Les obstacles et limitations à la vente via Internet (« problèmes de sécurité des paiements » et « incertitudes quant au cadre juridique des ventes sur Internet (par exemple contrats, conditions de livraison et garantie) »).
- Les pratiques de renforcement de la confiance pour le commerce sur Internet (« utilisation de marques de confiance », « mécanismes alternatifs de règlement des litiges (résolution via un tiers impartial) », « mécanismes pour le service clients et le traitement des plaintes »).

Certains pays européens, comme le Danemark et la Norvège, posent des questions plus détaillées dans leurs questionnaires nationaux. Ainsi le Danemark (2004) a posé plusieurs questions sur la sécurité informatique, notamment :

- Les mesures de sécurité informatique en vigueur.
- Le fait de savoir si elles ont été mises à jour au cours des trois mois précédents.
- La possibilité de communiquer avec l'entreprise par signature numérique/PIN, etc.
- La question de savoir si l'entreprise s'est informée sur la sécurité informatique.
- La mesure dans laquelle l'entreprise a connu un certain nombre de problèmes spécifiés (par exemple, accès non autorisé à des systèmes ou données).

L'Australie (en 2002-2003) a posé cinq questions spécifiques sur la sécurité informatique, à savoir :

- Les mesures de sécurité informatique en vigueur.
- Les problèmes spécifiques de sécurité informatique rencontrés.
- L'origine de ces incidents (interne, externe).
- Les conséquences de ces incidents.
- Les instances auxquelles ces incidents ont été signalés.

Le questionnaire de l'Australie comporte également une question sur les barrières à la vente sur Internet, qui propose parmi les réponses les « problèmes de sécurité ».

Dans ses questionnaires (2003 et années antérieures), le Canada a demandé si le site Web de l'entreprise était sécurisé et s'il comportait une charte de protection de la vie privée. Il comportait également une question sur les obstacles au commerce électronique proposant parmi les réponses la catégorie « Problèmes de sécurité ».

L'enquête japonaise sur les tendances en matière d'usage des télécommunications dans les entreprises (2003) comportait des questions sur :

- Les préjudices causés en relation avec les réseaux.
- Les mesures prises pour protéger la sécurité des données et des réseaux.
- La fréquence des mises à jour des fichiers de définition de virus.
- Les mesures prises pour protéger les informations à caractère personnel.

Elle comporte également une question sur les problèmes associés à l'utilisation des réseaux informatiques qui mentionne notamment la sécurité informatique et autres causes de même nature, ainsi qu'une question similaire sur les problèmes associés au commerce électronique.

#### ***Enquêtes spécialisées sur la sécurité des technologies de l'information***

Le *Census Bureau* des États-Unis a procédé en 2001 à une enquête pilote sur la sécurité informatique (*Computer Security Survey*) et constaté que l'information était généralement disponible mais difficile à recueillir en raison des faibles taux de réponse. L'enquête était très détaillée et comportait notamment des questions sur l'infrastructure, les détournements de fonds, la fraude, le vol d'informations, les dénis de services, le sabotage, les virus et attaques similaires, les réseaux affectés et la notification des incidents.<sup>6</sup> Les données tirées de l'enquête n'ont pas été publiées, en raison des faibles taux de réponse.

#### ***Enquêtes sur l'utilisation des TIC auprès des ménages***

Des questions ont également été posées aux ménages mais le champ couvert est moins vaste que pour les entreprises. Les pays de la Commission européenne (via le questionnaire type d'Eurostat), le Japon et les États-Unis posent des questions dans ce domaine.

Le questionnaire d'Eurostat pour 2005 comporte des questions sur la sécurité informatique et sur d'autres thèmes liés à la confiance, notamment :

- Protection de l'équipement d'accès à Internet utilisé au foyer (programme antivirus et pare-feu).
- Mises à jour des logiciels de sécurité au foyer.
- Utilisation individuelle de méthodes d'authentification en ligne (mot de passe, identifiant personnel ou signature numérique).
- Problèmes de sécurité rencontrés par les utilisateurs (par exemple virus informatique, paiement frauduleux).
- Trois questions sur les obstacles au commerce électronique en relation avec la confiance, l'une adressée aux ménages (pourquoi le ménage ne dispose-t-il pas d'un accès à Internet) et deux aux particuliers (limitations et obstacles de l'achat sur Internet).

Les trois questions sur les obstacles à l'accès à Internet ont été également conservées dans le questionnaire 2006. Les autres questions, toutefois, ont été omises, Eurostat faisant état de difficultés de collecte.

Au Japon, l'enquête sur les tendances dans l'utilisation des communications par les ménages (2003) comporte un certain nombre de questions sur la confiance, notamment :

- Les préjudices subis par les internautes au cours des 12 derniers mois, en particulier infection par virus, courrier électronique non sollicité, accès non autorisé et diffamation sur le Web.
- Les contre-mesures prises pour se protéger des virus informatiques ou accès non autorisés, notamment logiciels antivirus, sauvegarde de fichiers de données, et utilisation d'un pare-feu.
- Une question sur les obstacles à l'achat sur Internet, portant sur différents aspects liés à la confiance tels que « je suis préoccupé par le fait de divulguer les informations de mes cartes de crédit ».
- Une question sur les obstacles à l'utilisation de l'Internet concernant les domaines d'insatisfaction tant pour les internautes que pour ceux qui n'utilisent pas Internet.

En 2003, les États-Unis ont adopté une approche différente, en posant des questions sur la façon dont était perçue la sécurité sur Internet : degré de préoccupation à l'idée de fournir des informations de caractère personnel (en comparant l'Internet et le téléphone) et préoccupations suscitées par le contenu auquel les enfants sont exposés sur Internet (par comparaison avec la télévision). Par rapport au téléphone, 49.8 % de l'ensemble des déclarants estimaient plus préoccupante la fourniture d'informations sur Internet. Quelque 42.4 % considéraient les deux comme équivalents et seulement 7.8 % étaient moins préoccupés par la fourniture d'informations sur Internet que par téléphone (annexe 1, tableau 1). Par rapport à la télévision, 70 % de l'ensemble des déclarants étaient davantage préoccupés par l'exposition des enfants aux contenus sur Internet (annexe 1, tableau 2).

### ***Exemples de données officielles***

On trouvera dans l'annexe 1 du présent rapport certaines des données disponibles sur la sécurité informatique recueillies et publiées par: le bureau australien de statistiques (*Business Use of Information Technology Survey*), Statistique Canada (enquête sur le commerce électronique et la technologie), Eurostat (enquête communautaire sur l'utilisation des TIC et du commerce électronique), le Japon (enquête sur les tendances en matière d'utilisation des communications) et le *Census Bureau* des États-Unis (*Current Population Survey, Computer and Internet Supplement*).

## **Évolutions futures : les enquêtes types de l'OCDE sur l'utilisation des TIC par les entreprises et les ménages**

### ***Enquête type auprès des entreprises***

L'enquête type de l'OCDE sur l'utilisation des TIC par les entreprises est en cours de révision, les changements devant être finalisés courant 2005. Il est proposé d'ajouter un module séparé sur les mesures de sécurité concernant les technologies de l'information que les entreprises ont mises en place (à la fin de la période de référence) et les incidents observés en matière de sécurité des TI (durant la période de référence). Cette enquête prolonge les activités de collecte analogues menées par certains pays membres, comme indiqué plus haut.

De plus, une question a été proposée sur la question de savoir si le site Web de l'entreprise comporte une notice exposant sa politique en matière de sécurité, sa charte en matière de vie privée, un label de sécurité ou un label de protection de la vie privée.

Les questions sur les obstacles à l'utilisation d'Internet dans l'enquête type actuelle comportent certaines rubriques sur la sécurité. L'enquête type révisée n'a qu'une question sur les obstacles (au commerce électronique) et celle-ci comprend des rubriques sur la sécurité, la vie privée et la confiance (voir l'annexe 2 pour plus de précisions).

Les questions de l'enquête type sont reproduites dans l'annexe 2 accompagnées d'une synthèse des commentaires reçus des pays membres sur ces questions et sur les thèmes qui pourraient être développés.

### *Enquête type auprès des ménages*

L'enquête type de l'OCDE sur l'utilisation des TIC par les ménages et particuliers est également en cours de révision, ses changements devant être finalisés en 2005. Il est proposé d'ajouter trois questions nouvelles (non centrales) sur des thèmes en relation avec la sécurité informatique.

L'enquête actuelle propose des questions sur les obstacles à Internet comportant des rubriques sur la sécurité et la vie privée, et celles-ci seront conservées.

Les questions types proposées ont été reproduites dans l'annexe 2 accompagnées d'une synthèse des commentaires reçus des pays membres sur ces questions et sur les thèmes qui pourraient être développés.

## **PARTIE 2 : STATISTIQUES SUR LA CONFIANCE DANS L'ENVIRONNEMENT EN LIGNE ÉMANANT DE SOURCES SEMI-OFFICIELLES ET PRIVÉES**

On dispose d'un volume croissant de statistiques émanant de sources semi-officielles et privées dans des secteurs liés à la confiance dans l'environnement en ligne. Le terme « semi-officiel » est utilisé ici pour désigner des statistiques émanant de gouvernements et organismes publics, mais non des bureaux statistiques nationaux. Les sources privées englobent toutes les autres données qui n'entrent pas dans les catégories des données officielles ou semi-officielles. C'est notamment le cas, par exemple, des statistiques industrielles produites par des entreprises fournissant des services et applications tels que logiciels antivirus. Les données émanant de sources tant semi-officielles que privées peuvent être issues d'enquêtes auprès d'utilisateurs et de spécialistes des TIC, des plaintes de consommateurs, de statistiques sur la criminalité ou la fraude ou de tout un ensemble de statistiques *ad hoc* générées par l'industrie ou par la communauté Internet sur des phénomènes spécifiques affectant la confiance dans l'environnement en ligne. Les sections qui suivent visent à donner un aperçu des données disponibles, avec quelques exemples couvrant l'ensemble de la zone de l'OCDE.

### **Enquêtes sur les perceptions, les opinions et les usages**

Plusieurs enquêtes ont été réalisées au cours des années récentes par des entités semi-officielles et privées concernant la confiance dans l'environnement en ligne. Deux initiatives majeures dans ce domaine ont été lancées par la Commission européenne (2004) et, pour les États-Unis, par le *Pew Internet & American Life Project* (2000). L'enquête de la Direction GOV de l'OCDE sur les organismes du secteur public assurant des services d'administration électronique, qui est réalisée dans le cadre de ses examens par les pairs des programmes nationaux d'administration électronique, est un autre exemple. L'enquête de l'OCDE est l'une des rares à enquêter sur les perceptions dans le secteur public, à l'échelle internationale, en relation avec la confiance.

#### ***L'enquête de la Direction GOV de l'OCDE sur l'administration électronique***

La Direction de la gouvernance publique et du développement territorial (GOV) de l'OCDE identifie l'évolution des besoins de la société et des marchés et aide les pays à adapter leurs systèmes de gouvernement et leurs politiques territoriales. La Direction GOV contribue à l'amélioration de la gouvernance du secteur public par des données et analyses comparatives, la définition et la promotion de normes, et la facilitation de la transparence et des examens par les pairs. Dans le cadre de ce processus, la Direction GOV procède à des examens par les pairs des programmes d'administration électronique des pays membres (le Mexique, la Finlande, la Norvège et le Danemark ont fait l'objet d'un examen à ce jour). Une partie du processus d'examen consiste à adresser un questionnaire aux organismes du secteur public du pays examiné. Deux questions du questionnaire portent directement sur les perceptions en relation avec la confiance dans la prestation des services publics dans l'environnement en ligne. Ces questions sont les suivantes :

(Question 3.5) Estimez-vous que les procédures en ligne dans votre organisation bénéficient d'un niveau de protection équivalent aux mêmes procédures hors ligne en ce qui concerne (a) la vie privée, (b) la sécurité et (c) la protection des consommateurs.

(Question 7.4) Les facteurs suivants limitent-ils la demande par les consommateurs de services en ligne assurés par votre organisation, et dans l'affirmative, quelle est leur importance (g) protection de la vie privée en ligne jugée moindre que dans le même service hors ligne, (f) protection de la sécurité en ligne jugée moindre que dans le même service hors ligne.

On dispose des résultats pour le Danemark. Ceux-ci montrent que les fonctionnaires danois considèrent que les services d'administration électronique proposés bénéficient d'un niveau de protection équivalent ou supérieur aux mêmes procédures hors ligne en ce qui concerne la vie privée, la sécurité et la protection des consommateurs (annexe 3, figure 1). Ils indiquent aussi les perceptions des fonctionnaires danois en ce qui concerne la vie privée et la sécurité en tant qu'obstacles à l'utilisation de l'administration électronique, et permettent des comparaisons avec d'autres domaines susceptibles d'être des obstacles (annexe 3, figure 2). En ce qui concerne la sécurité et la vie privée, plus de 60 % des déclarants indiquent que ces aspects ne constituent actuellement pas des contraintes à la prestation de services d'administration électronique. Un peu moins de 20 % considèrent que la sécurité et la vie privée sont un obstacle important ou très important, le reste estimant que ces facteurs ont une certaine importance.

### *L'eurobaromètre de la Commission européenne*

La Commission européenne suit l'évolution de l'opinion publique dans les États membres depuis 1973. Les enquêtes et études, réalisées par le Groupe de recherche sur l'opinion européenne, portent sur une diversité de thèmes en relation avec la citoyenneté européenne : élargissement, situation sociale, santé, culture, technologies de l'information, environnement, euro, défense, etc. Ces études sont disponibles sur le site Web du secteur Analyse de l'opinion publique de la Commission européenne.<sup>7</sup>

En 2003, la Direction générale « Santé et protection des consommateurs » a demandé une enquête spéciale Eurobaromètre sur l'opinion publique à l'égard du commerce électronique. Cette enquête, « *European Union Public Opinion on Issues Relating to Business to Consumer E-commerce* » (référence : 201 EB60.0) a été réalisée en septembre 2003.<sup>8</sup>

Cette étude ponctuelle visait essentiellement à sonder l'opinion publique communautaire sur les questions liées au commerce électronique en demandant aux citoyens de l'UE comment ils percevaient la sécurité sur Internet et quelles étaient leurs préoccupations à cet égard. L'enquête répartissait les déclarants en deux catégories : ceux qui avaient utilisé l'Internet pour le commerce électronique (16 %) et ceux qui n'avaient jamais utilisé l'Internet pour le commerce électronique (83 %). Des questions étaient ensuite posées aux déclarants, dans les deux catégories (annexe 3, tableaux 1 et 2).

En 2003, la principale raison invoquée par les citoyens de l'UE pour ne pas effectuer d'achats sur Internet étaient qu'ils n'avaient pas accès à Internet (57 %). Les problèmes de sécurité ne venaient qu'au troisième rang (25 %), après le fait de ne pas être intéressé par un quelconque achat sur Internet (28 %). En revanche, la sécurité des paiements était la préoccupation première des citoyens de l'UE qui avaient accès à l'Internet (48 %). Parmi les autres questions liées à la confiance, figuraient : la possibilité d'obtenir un remboursement (38 %), la livraison (36 %) et la crédibilité de l'information sur Internet (27 %).

### *Eurobaromètres sur la sécurité et la vie privée*

Il faut noter que l'enquête Eurobaromètre comportait des questions spécifiques sur la sécurité et la vie privée. Il était demandé aux déclarants s'ils avaient entendu parler des « marques de confiance Internet », de notices sur la sécurité des paiements et des notices sur la protection des données de caractère personnel (annexe 3, tableaux 3, 4 et 5). Des questions sur ces points peuvent éclairer les décideurs sur la sensibilisation du public à l'égard de certaines des principales mesures de protection pour renforcer la confiance.

Les « marques de confiance Internet » sont des sceaux ou labels apposés sur les sites Web de commerce électronique. Ils indiquent, par exemple, que le commerçant en ligne a choisi SSL ou une autre solution de traitement des paiements pour protéger la communication des informations de la carte de crédit ou d'autres informations confidentielles. L'enquête Eurobaromètre a montré que le grand public connaissait généralement mal ce concept, 10 % seulement des déclarants, en moyenne sur l'ensemble de la zone de l'UE, ayant entendu parler de marques de confiance. Sur ces 10 %, un peu plus de la moitié (56 %) avaient noté de telles marques sur des sites Web qu'ils avaient visités. Un peu moins de la moitié (49 %) de ceux ayant entendu parler des marques de confiance considéraient qu'elles rendaient les sites Web plus fiables. Dans l'enquête Eurobaromètre il était également demandé aux déclarants s'ils étaient davantage ou moins susceptibles de faire confiance aux marques de confiance nationales ou étrangères. Quelque 18 % des personnes interrogées dans l'ensemble de la zone de l'UE ont déclaré qu'elles feraient davantage confiance à des marques originaires d'un autre pays que le leur. Une proportion légèrement supérieure (21 %) toutefois, était d'avis contraire et considérait que les marques de confiance « étrangères » susciteraient moins de confiance.

Bien que les notices sur la sécurité sur les paiements (21 %) et notices sur la vie privée (24 %) soient mieux connues, dans l'ensemble de la zone de l'UE, leur taux de reconnaissance reste faible. Toutefois, comme les marques de confiance, ces mesures de protection sont mieux connues de ceux qui ont accès à Internet ou effectuent des achats sur Internet que dans la population générale.

Un eurobaromètre spécial a également été réalisé en 2003 pour évaluer les opinions des citoyens de l'UE sur la protection des données.<sup>9</sup> À l'époque, il est ressorti de l'enquête que 72 % des déclarants n'avaient pas entendu parler d'outils ou de technologies destinés à limiter le recueil de données les concernant lorsqu'ils utilisent l'Internet (technologies dites de protection de la vie privée ou PET). Seuls 6 % des déclarants signalaient utiliser de tels outils. Quelque 30 % des personnes ayant entendu parler de ces outils et technologies mais ne les utilisant pas déclaraient qu'elles ne pensaient pas avoir les compétences suffisantes pour le faire.

### *Enquêtes par l'industrie*

Les enquêtes effectuées par l'industrie sont une autre source d'information sur les perceptions du public concernant la confiance dans l'environnement en ligne. On peut ainsi mentionner une enquête réalisée par Harris Interactive, pour le compte de Verisign, en septembre 2004.<sup>10</sup> Selon cette enquête, 31 % des Américains citent les problèmes de sécurité comme un facteur clé les dissuadant d'effectuer davantage d'achats en ligne.<sup>11</sup> Les frais d'expédition (48 %) et l'impossibilité de manipuler un article avant de l'acheter (46 %) sont mentionnés comme les principaux obstacles, suivis par la difficulté pour retourner les articles.<sup>12</sup>

Bien que ces résultats ne soient non directement comparables avec ceux de l'enquête Eurobaromètre, les marques de confiance semblent mieux connues aux États-Unis. Il ressort de l'enquête Interactive Harris que 74 % des personnes aux États-Unis ayant effectué au moins un achat en ligne recherchent la présence d'une marque de confiance pour décider d'effectuer ou non un achat sur un site de commerce électronique.<sup>13</sup> Cela s'explique toutefois peut-être par le rôle important joué par les notices de politique en matière de vie privée et les marques de confiance dans l'approche réglementaire des États-Unis à l'égard de la vie privée. Il se peut par contre que les déclarants de l'Union européenne n'aient pas confiance dans le fonctionnement de l'approche par législation-cadre pour la protection de la vie privée dans les États membres de l'Union. Un autre résultat méritant d'être mentionné est que seulement 28 % des acheteurs en ligne interrogés par Harris Interactive avaient entendu parler du « hameçonnage ».

En septembre-octobre 2004, l'une des enquêtes les plus remarquables entreprises sur l'utilisation de mesures de protection en ligne a été réalisée par AOL et la *National Cyber Security Alliance* (NCSA).<sup>14</sup>

Dans cette enquête, des internautes disposant soit de connexions à haut débit soit de connexions par réseau commuté ont été interrogés avant que le disque dur de leur ordinateur personnel ne soit analysé. Parmi les questions ainsi posées préalablement, il leur était demandé dans quelle mesure ils considéraient que leur ordinateur était protégé des virus, des pirates et des menaces en ligne et s'ils utilisaient leur connexion au foyer pour des transactions sensibles ou s'ils stockaient des informations sensibles. Des questions leur étaient posées concernant leur utilisation d'outils de protection (par exemple, pare-feu, logiciel antivirus, anti logiciel espion), puis leur ordinateur était analysé pour voir dans quelle mesure leurs réponses correspondaient à la réalité. Dans certaines catégories, les écarts étaient considérables entre les perceptions et les résultats de l'analyse. Parmi les utilisateurs se protégeant contre les virus, 71 % déclaraient faire des mises à jour quotidiennes ou hebdomadaires. Or, l'analyse de l'ordinateur montrait que 67 % des programmes antivirus n'avaient pas été mis à jour depuis une semaine. Il existait également de fortes divergences en ce qui concerne les logiciel espions quant à ce que les utilisateurs croyaient avoir sur leur ordinateur ou dont ils pensaient avoir autorisé l'installation, et ce que montrait l'analyse du disque dur. Quelque 53 % des utilisateurs interrogés pensaient leur machine infestée par des logiciel espions ou des logiciels publicitaires, alors que l'analyse révélait que de tels programmes étaient installés sur 80 % des machines.

L'une des enquêtes permanentes les plus anciennes réalisées par le secteur privé sur les opinions des consommateurs à l'égard des systèmes de paiement sur Internet est celle de l'Université de Karlsruhe en Allemagne. Réalisée pour la première fois en 1998, elle est appuyée par des entreprises comme Deutsche Telekom, FirstGate Internet et WEB.DE. Les résultats les plus récents au moment de la rédaction du présent rapport ont été publiés en novembre 2004.<sup>15</sup> Parmi les questions posées figuraient celle de savoir à quels types d'entités les consommateurs faisaient confiance pour la prestation de système de paiement en ligne. En 2004, les déclarants ont répondu dans l'ordre : banques (84.4 %), sociétés de cartes de crédit (59 %), FAI (17.1 %), opérateurs de télécommunications (14 %), tiers indépendants (12.2 %) et sans préférence (10.9 %).

### *Enquêtes de l'industrie sur les usages d'Internet*

Une question intéressante dans l'évaluation de la confiance dans l'environnement en ligne est de savoir dans quelle mesure les internautes sont disposés à autoriser la réutilisation de leurs informations personnelles en échange d'autres avantages. Une étude universitaire réalisée en 2005, par exemple, a consisté à effectuer une expérience avec enchères sous pli scellé pour voir quelle valeur monétaire les utilisateurs associaient aux « informations privées concernant leur localisation » dans les services mobiles.<sup>16</sup>

Un certain nombre d'entreprises étudient les comportements de panels d'internautes volontaires. En échange, ces internautes peuvent bénéficier d'incitations financières directes, telles que réductions ou accès à des services (par exemple, accès gratuit à des mises à jour de logiciels antivirus). Ce suivi, parfois appelé « researchware », peut être une source commerciale très utile d'informations sur les usages en ligne, notamment pour éclairer les problèmes liés à la confiance.<sup>17</sup> Les résultats sont également disponibles par pays, ce qui permet des comparaisons internationales, bien que de source privée.

Une question qui commence toutefois à se poser dans l'utilisation des « researchware », est de savoir jusqu'à quel point certaines entreprises en ligne sont disposées à autoriser la surveillance de leurs clients par des tiers, compte tenu de leurs propres préoccupations de sécurité. En Australie et en Nouvelle-Zélande, par exemple, certaines banques ont commencé à bloquer l'accès de leurs services bancaires en ligne aux utilisateurs ayant installé sur leur ordinateur des logiciels de surveillance de sociétés tiers.<sup>18</sup> Les banques en question ont fait savoir que ces logiciels de recherche de sociétés tierces constituent une violation des conditions d'utilisation de leurs services bancaires par Internet.

### ***Le Pew Internet & American Life Project***

Le *Pew Internet & American Life Project* est un centre de recherche sans but lucratif qui étudie les effets sociaux de l'Internet aux États-Unis. En 2000, le *Pew Internet & American Life Project* a entrepris une étude appelée « *Trust and Privacy On-line: Why Americans Want to Rewrite the Rules* ». <sup>19</sup> Les résultats de l'enquête ont mis en évidence chez les internautes tout un ensemble de préoccupations, allant de l'accès aux informations personnelles jusqu'à l'interception ou le suivi des communications (annexe 3, tableau 6). Une comparaison des résultats avec ceux d'une étude *Pew* antérieure réalisée en 1998 a fait ressortir une préoccupation croissante concernant la vie privée et les virus (annexe 3, tableau 7). L'enquête a montré qu'environ la moitié de l'ensemble des internautes connaissaient l'existence des « cookies » mais que seul un pourcentage relativement limité d'utilisateurs bloquaient leur utilisation (annexe 3, tableau 8). Un « cookie » est un petit fichier de données qui peut être stocké sur le disque dur de l'ordinateur de l'internaute pour une multitude d'utilisations différentes, comme le stockage d'informations concernant l'utilisateur utiles pour un site Web, par exemple personnalisation des préférences de l'utilisateur ou suivi du comportement de l'utilisateur sur un ou plusieurs sites Web.

### ***Consumer Reports***

*Consumer Reports* est publié par la *Consumers Union*, qui est un groupe indépendant d'informations et de défense des consommateurs aux États-Unis. En août 2005, *Consumer Reports* a publié les résultats d'une enquête représentative au plan national conduite auprès de plus de 3 200 ménages disposant d'un accès Internet à domicile. <sup>20</sup> L'une des conclusions était qu'un tiers des déclarants indiquaient qu'un virus ou un logiciel espion avait provoqué de sérieux problèmes sur leur système informatique et/ou des pertes financières au cours des deux années précédentes. Sur la base de l'enquête 2005, *Consumer Reports* a commencé à compiler un tableau annuel de l'état du Net (« State of the Net ») visant à évaluer la probabilité et l'impact de quatre dangers majeurs en ligne. Le rapport 2005 identifiait le spam, les virus, les logiciels espions et l'hameçonnage comme représentant les principales menaces, il évaluait s'ils allaient évoluer favorablement ou défavorablement et présentait des données sur leur incidence, le coût moyen par incident et le coût total à l'échelle du pays.

### **Enquêtes réalisées par des professionnels de la sécurité et des organismes chargés de l'application des lois**

L'enquête annuelle sur la criminalité et la sécurité informatique du *Computer Security Institute* et du *Federal Bureau of Investigation (CSI/FBI)* est sans doute l'étude la plus vaste et la plus complète de ce type. En 2004, l'étude a enregistré les réponses de 494 praticiens de la sécurité informatique aux États-Unis appartenant à des entreprises, des organismes fédéraux, des institutions financières, des institutions médicales et des universités. <sup>21</sup> L'enquête comporte toute une série de questions touchant la sécurité, notamment l'évaluation des pertes liées à différents types d'incidents. En 2004, sur un montant total de USD 141 millions notifié par les déclarants, les attaques par virus et dénis de service sont celles qui ont causé les plus fortes pertes. L'enquête CSI/FBI demande également aux déclarants de chiffrer leurs dépenses de sécurité, en pourcentage de leurs dépenses totales dans le secteur des TI. En 2004, 46 % des déclarants ont indiqué que leurs organisations allouaient entre 1 et 5 % de leur budget informatique total à la sécurité. L'enquête donne également des informations sur un certain nombre d'indicateurs, notamment les dépenses de sécurité par employé, le montant du budget total de sécurité externalisé et la question de savoir si les organisations évaluent le retour sur investissements de leurs dépenses de sécurité.

L'enquête « E-Crime Watch Survey » est conduite auprès de responsables de la sécurité et de l'application des lois par la revue CSO, en coopération avec l'*United States Secret Service* et le centre de coordination des *Computer Emergency Response Team (CERT)* au *Software Engineering Institute* de l'Université Carnegie Mellon. Le montant des pertes dues à la criminalité informatique indiqué par les

déclarants à l'enquête 2004 s'élève à USD 666 millions pour 2003.<sup>22</sup> Il est également demandé aux déclarants de donner une évaluation chiffrée des pertes dans leur secteur liées par exemple aux pertes d'exploitation, aux pertes financières, etc. En 2004, il est ressorti de l'enquête que 32 % des déclarants ne cherchaient pas à retracer les pertes dues à la criminalité informatique ou aux intrusions et que parmi ceux qui suivent l'évolution de cet indicateur, environ la moitié ignorent leurs pertes totales.

En 2005, le *Department of Homeland Security* et le *Department of Justice* des États-Unis se proposent d'interroger 36 000 entreprises pour examiner la nature et la fréquence des incidents de sécurité informatique. Le but de cette étude est d'améliorer les données sur la cybercriminalité afin d'aider à l'analyse des mesures prises par le gouvernement et le secteur privé et de disposer de données nationales statistiquement significatives sur la cybercriminalité dans l'ensemble des entreprises aux États-Unis, notamment celles appartenant à des secteurs caractérisés par des infrastructures critiques.

En Australie, l'AusCERT procède à une « Computer Crime and Security Survey » annuelle, adaptée de l'enquête CSI/FBI du même nom.<sup>23</sup> Cela permet des comparaisons des tendances entre les deux enquêtes. Le questionnaire est adressé aux spécialistes de la sécurité des 350 plus grosses entreprises australiennes (y compris les institutions gouvernementales et éducatives). En 2004, il y a eu 199 réponses (83 %). Cette enquête permet notamment d'obtenir une évaluation chiffrée des pertes de temps et des pertes financières imputables à la criminalité informatique. En 2004, les pertes totales signalées par les déclarants se sont élevées à USD 12.6 millions, contre un peu moins de USD 5 millions en 2002.

Au Royaume-Uni, le *Department of Trade and Industry* parraine l'enquête « Information and Security Breaches Survey ». Celle-ci est destinée à établir des comparaisons entre la situation au Royaume-Uni et les résultats de l'enquête CSI/FBI aux États-Unis.<sup>24</sup> Toujours au Royaume-Uni, la *National Hi-Tech Crime Unit* parraine également des enquêtes auprès des entreprises sur la prévalence et l'impact de la criminalité informatique.<sup>25</sup> En 2003, les atteintes les plus fréquentes en matière de criminalité informatique ont été les attaques par virus et les attaques par déni de services. Les pertes totales, pour les 167 entreprises interrogées dans l'enquête 2003, ont été chiffrées à USD 365 millions, la majeure partie (62 %) étant imputable à des cas de fraude financière. Dans son enquête 2004, la *National Hi-Tech Crime Unit* a estimé le coût total de la criminalité informatique dans les entreprises britanniques à USD 4.5 milliards.<sup>26</sup>

En Allemagne, l'Office fédéral pour la sécurité de l'information procède chaque année à une étude pour renforcer la sensibilisation à l'égard des produits qu'il propose. Des responsables de la sécurité informatique, des responsables de la protection des données et des journalistes sont interrogés dans le cadre d'enquêtes représentatives. En 2004, une étude sur la sensibilisation a également été réalisée auprès de groupes cibles de particuliers utilisateurs de PC. Les résultats sont étudiés en relation avec la planification des projets de l'Office fédéral pour la sécurité de l'information. Des sondages d'opinion sont également prévus auprès d'experts et de particuliers.

En Finlande, le ministère des Finances publie une étude annuelle sur l'utilisation des TIC dans la fonction publique.<sup>27</sup> Le ministère des Finances procède à ces études depuis 1975 dans le cadre de sa mission d'orientation et de gestion des activités de la fonction publique dans le domaine des TIC et de la sécurité de l'information. La publication comprend des informations statistiques sur les dépenses totales dans le domaine des technologies de l'information, sur les effectifs dans le secteur des technologies de l'information, sur les équipements des technologies de l'information et sur la gestion de l'information, ainsi que sur la sécurité de l'information dans les organismes publics. D'autres informations sur cette étude, ainsi que les indicateurs disponibles sont exposés dans l'encadré 1.

En Espagne, l'Association espagnole des entreprises d'électronique et de communication (ASIMELEC) a procédé à une étude centrée sur la sécurité des TIC dans les secteurs des technologies des télécommunications et de l'information en Espagne.<sup>28</sup> L'objectif de cette étude était d'analyser le niveau de

connaissances et d'investissement en matière de sécurité dans l'industrie espagnole des TI et des communications. Cette étude a conclu à une insuffisance du niveau de sécurité de l'information et de sensibilisation des entreprises au besoin de sécurité en ligne. Elle a mis en évidence le fait que seuls les logiciels antivirus et les pare-feu étaient largement utilisés parmi les entreprises espagnoles.

Les enquêtes réalisées par les professionnels de la sécurité et des TIC sont une source complémentaire de données. Symantec, qui est un éditeur de logiciels de sécurité, a procédé à un certain nombre d'enquêtes auprès de spécialistes de la sécurité sur les actions que ceux-ci mettent en œuvre en matière de sécurité et de vie privée. Un des premiers exemples en la matière a été une étude de l'utilisation respective des pare-feu par le grand public et les professionnels des TI.<sup>29</sup> Un autre exemple est une étude comparative en 2004 des attitudes et comportements en matière de vie privée des spécialistes de la sécurité aux États-Unis, au Royaume-Uni et dans d'autres pays de l'Union européenne.<sup>30</sup>

Des entreprises comme Deloitte Touche Tohmatsu réalisent des études auprès de spécialistes de la sécurité dans des domaines comme les services financiers.<sup>31</sup> Parmi les questions posées figure notamment celle de savoir si les entreprises considèrent la sécurité comme un domaine pouvant représenter un avantage concurrentiel, la description des structures de notification interne et les tendances dans les niveaux d'investissement. Dans la région nordique, la direction de PLS RAMBOLL a procédé à une enquête auprès d'entreprises de commerce électronique.<sup>32</sup> L'étude a notamment bénéficié d'un soutien financier du Conseil nordique des ministres. Outre les questions de sécurité, l'enquête rend compte du respect de la législation en vigueur concernant par exemple la protection des données, les règles en matière de marketing, etc.

Encadré 1 : **Enquête sur l'utilisation des TIC dans l'administration publique en Finlande, sécurité et indicateurs sur la confiance en ligne**

Parmi les organismes publics fournissant des informations pour l'enquête annuelle sur l'utilisation des TIC, figurent notamment des ministères et des organismes administratifs financés sur le budget de l'État. Au total, ces entités emploient quelque 123 000 personnes, dans 2 606 unités différentes. En 2004, la dépense totale consacrée aux TIC dans ces organismes gouvernementaux a été de EUR 588 millions. Le nombre total de personnels informatiques à plein temps dans ces organismes, fin 2004, était d'environ 4 000. La proportion de personnels de TI dans les effectifs totaux des organismes gouvernementaux était de 3 %. Fin 2004, on dénombrait 160 828 ordinateurs personnels dans les organismes gouvernementaux en Finlande, soit 1.3 poste de travail par personne. Quelque 16 000 stations de travail étaient mises à la disposition du public. On dénombrait également 3 433 serveurs de fichiers et d'impression. Le nombre de bases de données multi-utilisateurs et de serveurs d'application était de 4 840. En 2004, l'enquête a montré que toutes les organisations disposaient d'un site Web, que 78 % proposaient des formulaires électroniques sur Internet et que la moitié proposaient des services au public.

L'enquête 2004 a fait ressortir des évolutions positives dans différents domaines de la sécurité de l'information en Finlande parmi les utilisateurs du secteur public. Un certain nombre d'exemples ont été mis en évidence en matière de sécurité de l'information administrative et technique, d'instructions et de plans de sécurité de l'information, de coopération entre unités, de protection de la vie privée, de protection contre les attaques/virus et de plans de secours. En particulier, parmi les organisations participant aux projets en coopération pilotés par le ministère des Finances et le Conseil de gestion de la sécurité de l'information et de gouvernement (VAHTI) des développements et impacts significatifs ont été relevés. Ces développements sont mesurés au moyen d'un certain nombre d'indicateurs.

- Pourcentage d'organisations ayant un *plan de gestion des technologies de l'information*.
- Pourcentage d'organisations ayant des *plans de sécurité de l'information* ainsi que pourcentage d'organisations ayant des *plans de secours*.
- Pourcentage d'organisations dotées d'une *personne chargée de la sécurité informatique*. Pourcentage d'organisations dans lesquelles cette personne *rend compte à la direction générale*.
- Pourcentage d'organisations dotées d'un *organisme de coordination pour la sécurité de l'information au sein de plusieurs unités*.
- Pourcentage d'organisations dont les *instructions en matière de sécurité de l'information* couvrent l'ensemble des domaines importants en la matière.
- Pourcentage d'organisations dotées d'une *politique en matière de courrier électronique acceptée par la haute direction et communiquée au personnel*.
- Pourcentage d'organisations publiant des *descriptifs des registres en ligne sur leurs pages Web*.
- Pourcentage d'organisations dont la *politique en matière de protection de la vie privée est publiée sur leur site Web*.
- Autres indicateurs : *participation à des actions de coopération internationale en matière de sécurité des TIC*.
- La quasi-totalité des organisations utilisent un *système antivirus sur l'ensemble de leurs ordinateurs*.
- La quasi-totalité des organisations vérifient l'absence de virus dans le courrier électronique avant de le distribuer aux destinataires.
- Autres mécanismes mis en oeuvre : *cryptographie dans différents domaines ; IDS : en usage, prévu/non*.

L'enquête comportait également des questions sur les problèmes posés par les atteintes de sécurité, les programmes de virus, etc., tels que :

- *Pourcentage d'organisations dans lesquelles des attaques de sécurité informatique externes ont motivé l'adoption d'actions spécifiques au cours des 12 derniers mois*.
- *Pourcentage d'organisations dans lesquelles, pour cause de virus, un système ou une partie de système a été rendu non opérationnel pour une durée quelconque au cours des 12 mois précédents*.

Il est en général demandé aux déclarants de répondre « en usage », « prévu », ou « néant » en ce qui concerne les applications d'administration électronique et la sécurité des applications d'administration électronique interactive pour les indicateurs suivants :

- Pourcentage d'organisations disposant d'un *service propre interactif d'administration électronique opérationnel* et pourcentage d'organisations qui prévoient un projet de cette nature.
- Pourcentage d'organisations utilisant un système à *clé publique ou par signature numérique pour leurs applications d'administration électronique interactives*. Pourcentage d'organisations ayant en projet ce type de services.
- Pourcentage d'organisations appliquant une *norme d'authentification fondée sur mot de passe unique pour leurs applications interactives d'administration électronique (normes utilisées dans un premier temps dans le secteur bancaire et désormais largement utilisées dans différents secteurs)*. Pourcentage d'organisations ayant en projet ce type de services.
- Pourcentage d'organisations dont les *services d'administration électronique interactifs sont accessibles sur mobile* et pourcentage d'organisations offrant à leurs administrés un moyen d'acquiescer en ligne leurs services d'administration électronique interactifs.

## Statistiques sur les plaintes des consommateurs et les fraudes sur Internet

Les données sur les plaintes des consommateurs offrent une source d'informations sur les problèmes en relation avec le commerce électronique. Aux États-Unis, un certain nombre de centres recueillent les plaintes concernant les sites Web. L'un d'entre eux, *Consumer Sentinel*, géré par la *Federal Trade Commission* (FTC), a une vocation internationale et c'est celui qui couvre le plus grand nombre de plaintes. Par ailleurs, *Consumer Sentinel* propose des définitions des éléments qu'il s'attache à mesurer, chose qui n'est pas toujours évidente sur d'autres sites Web dont l'information méthodologique sur les statistiques présentées est souvent très limitée, voire absente. Une observation qui se retrouve sur l'ensemble des sites Web étudiés est que la catégorie de plaintes qui vient en tête est presque inmanquablement la fraude en relation avec les enchères sur Internet et que le nombre de plaintes déposées augmente au fil du temps.

### *Consumer Sentinel*

La base de données de *Consumer Sentinel*, gérée par la *Federal Trade Commission*, contient plus d'un million de plaintes pour fraude déposées par des consommateurs auprès d'organismes fédéraux, d'État et locaux et d'organismes privés.<sup>33</sup> En ligne depuis 1997, *Consumer Sentinel* vise à faciliter l'échange d'informations de manière à renforcer et rendre plus efficace l'application des lois. Projet conjoint international multi-agences, *Consumer Sentinel* contribue également à l'éducation des consommateurs et aux efforts de prévention à l'étranger.

Les plaintes peuvent être classées en deux catégories : les plaintes pour vol d'identité et les plaintes pour fraude. Les plaintes pour fraude peuvent elles-mêmes être subdivisées en plaintes pour fraude sur Internet et les plaintes pour d'autres types de fraude. Les plaintes pour fraude sur Internet ont sensiblement augmenté ces dernières années passant de 55 727 en 2001 à 166 617 en 2003 (annexe 3, figure 3). En 2003, les enchères sur Internet ont été la principale source de plaintes pour fraude (annexe 3, figure 4). Ces chiffres ne comprennent pas les cas de vol d'identité, qui peuvent être perpétrés via Internet, mais pour lesquels il n'existe pas de données distinctes. Une plainte pour fraude est considérée comme liée à Internet si elle concerne un produit ou service sur Internet, si l'entreprise contacte initialement le client via Internet ou si le consommateur répond via Internet.

*Consumer Sentinel* suit également l'évolution à long terme des fraudes transfrontières. Une plainte pour fraude est considérée comme « transfrontière » si : *i*) un consommateur aux États-Unis se plaint d'une entreprise située au Canada ou dans un autre pays étranger, *ii*) un consommateur canadien se plaint d'une entreprise située aux États-Unis ou dans un autre pays étranger, ou *iii*) un consommateur d'un pays étranger se plaint d'une entreprise située aux États-Unis ou au Canada. L'implantation de l'entreprise est déterminée par les adresses signalées par les plaignants et donc cette information sous-estime le nombre de plaintes transfrontières. Dans certains cas, l'adresse de l'entreprise fournie par le consommateur peut de fait n'être qu'une boîte à lettres, et non pas l'implantation physique de l'entreprise, et dans d'autres cas, le consommateur ignore si celle-ci est localisée aux États-Unis ou à l'étranger. Le nombre de plaintes transfrontières, notifiées par *Consumer Sentinel*, est passé de 5 225 en 2001 à 21 181 en 2003 (annexe 3, figure 5). Ces chiffres sont également disponibles par lieu d'implantation (annexe 3, tableau 9).

### *Internet Fraud Complaint Center*

L'*Internet Fraud Complaint Center* (IFCC) est un partenariat entre le *Federal Bureau of Investigation* (FBI) et le *National White Collar Crime Center* (NW3C).<sup>34</sup> La mission de l'IFCC est de s'attaquer aux fraudes commises sur Internet. L'IFCC fournit un mécanisme de notification qui alerte les autorités, aux États-Unis, en cas de suspicion de délit civil ou pénal. Pour les organismes chargés de faire appliquer les lois et ceux qui ont une mission de réglementation à tous les niveaux, l'IFCC permet de centraliser les

plaintes relatives à la fraude sur Internet, de recenser les mécanismes de fraude et de disposer de données statistiques sur les tendances actuelles en matière de fraude. Des statistiques de l'IFCC sont disponibles dans les rapports annuels sur la fraude sur Internet de même que dans des rapports traitant plus spécifiquement de la fraude aux enchères sur Internet.<sup>35</sup> Les données publiées par l'IFCC font ressortir les mêmes tendances que les chiffres de *Consumer Sentinel*. Les cas de fraude sur Internet augmentent, et la fraude aux enchères sur Internet en est la première cause (annexe 3, figures 6 et 7).

### ***National Fraud Information Center et Internet Fraud Watch***

Le NFIC a été créé en 1992 par la *National Consumers League*, organisation sans but lucratif de défense des consommateurs aux États-Unis, chargée de lutter contre la menace croissante de la fraude par télémarketing par une action renforcée de prévention et de sanction.<sup>36</sup> En 1996, l'*Internet Fraud Watch* été lancé, pour permettre au NFIC d'offrir aux consommateurs des conseils sur les promotions dans le cyberspace et d'orienter les signalements de suspicion de fraude en ligne et sur Internet vers les organismes gouvernementaux compétents.

Le NFIC recueille également les plaintes de fraude sur Internet, il compile des données et les rend disponibles sur son site Web. Le nombre total de plaintes enregistrées par le NFIC est beaucoup plus faible (37 183 plaintes en 2003) que par *Consumer Sentinel* et l'IFCC. Cela s'explique notamment par le fait que son champ d'activité est beaucoup plus restreint géographiquement (États-Unis uniquement) que certains des autres centres de plainte. En 2004, les enchères sur Internet ont été une fois de plus la principale source de plaintes des consommateurs, devant la non-distribution des produits commandés et la fraude dite « des scams africains » ou « fraude 419 ».<sup>37</sup> Il convient de noter que le hameçonnage ou « phishing » occupe la quatrième place dans la liste des escroqueries sur Internet en 2004, alors qu'il était absent de cette même liste en 2003.<sup>38</sup>

### ***Econsumer.gov***

En 2001, pour répondre aux défis de la fraude multinationale sur Internet et attachés à renforcer la protection et la confiance des consommateurs dans le commerce électronique, 13 pays ont inauguré *econsumer.gov*, qui est une initiative commune pour recueillir et échanger les plaintes en matière de commerce électronique transfrontières.<sup>39</sup> En 2004, le projet réunissait les organismes de protection des consommateurs de 19 pays : Australie, Belgique, Canada, Corée, Danemark, États-Unis, Finlande, Hongrie, Irlande, Japon, Lettonie, Lituanie, Mexique, Norvège, Nouvelle-Zélande, Pologne, Royaume-Uni, Suède et Suisse.

Le projet comporte deux éléments : un site Web public multilingue, et un site Web protégé par mot de passe, réservé aux pouvoirs publics. Le site public fournit des informations générales sur la protection des consommateurs dans l'ensemble des pays appartenant au RICPC (réseau international de contrôle et de protection des consommateurs), des informations pour contacter les autorités de protection des consommateurs dans ces pays, et un formulaire de plainte en ligne.<sup>40</sup> Toutes les informations sont disponibles en anglais, en français, en allemand et en espagnol. Grâce au réseau mis en place par *Consumer Sentinel*, les plaintes déposées sont mises en commun avec les autorités de protection des consommateurs participantes, via le site Web réservé aux pouvoirs publics. Le site Web fournit également des statistiques, notamment sur la fraude transfrontières via Internet.<sup>41</sup>

### **Ventes de détail, sécurité et fraude en ligne**

Dans le rapport 2004 de Symantec sur la sécurité sur Internet, le commerce électronique est cité comme le secteur ayant été le plus fréquemment ciblé par les fraudeurs durant le premier semestre de l'année, avec près de 16 % d'attaques considérées comme délibérées à l'encontre de sites de commerce

électronique, contre 4 % les six mois précédents.<sup>42</sup> À l'époque, Symantec signalait que cela indiquait peut-être une évolution dans les motivations des pirates, ceux à la recherche de notoriété cédant la place à des criminels professionnels à la recherche de gains financiers illicites. Cela peut aussi refléter en partie l'utilisation et l'importance croissantes du commerce électronique.

Bien qu'encore faible comparé au volume global des ventes de détail, le volume du commerce électronique progresse dans l'ensemble de la zone de l'OCDE. Aux États-Unis, le volume des ventes de détail en ligne a triplé entre 1999 et 2004.<sup>43</sup> Les chiffres publiés par la profession dénotent également une progression du commerce électronique. En 2003, les titulaires de cartes Visa en Europe ont dépensé plus de USD 14 milliards dans le cadre de transactions de détail en ligne, soit le double de l'année précédente.<sup>44</sup> Ce chiffre représente 1.5 % des dépenses totales des détenteurs européens de cartes Visa en 2003. Au Royaume-Uni, l'*Association for Payment and Clearing Services* (APACS) a indiqué qu'en avril 2004 un paiement sur dix par carte de crédit s'effectuait désormais en ligne.<sup>45</sup> La même année, l'APACS indiquait également que 22 millions d'internautes au Royaume-Uni effectuaient soit des achats, soit des opérations bancaires en ligne, la moitié d'entre eux effectuant les deux. Selon l'APACS, 6.7 millions d'acheteurs en ligne ont effectué chacun en moyenne 6.5 achats en 2000. En 2003, le nombre d'acheteurs en ligne avait triplé et chacun effectuait en moyenne 11.2 achats en ligne.

Il n'y a que peu de données disponibles publiquement sur les coûts financiers de la fraude ou des atteintes à la sécurité en relation avec l'activité de vente au détail en ligne. Visa rend compte, sur une base trimestrielle, du montant total de la fraude sur l'ensemble des transactions effectuées par les détenteurs de ses cartes. Ces données n'explicitent pas le montant correspondant à la fraude en ligne. En juin 2004, les transactions frauduleuses ont représenté 0.05 % du volume total des transactions Visa aux États-Unis.<sup>46</sup> Ce chiffre a régulièrement baissé, par rapport aux 0.18 % du total des transactions en 1992.<sup>47</sup> MasterCard ne fait pas de commentaires sur les statistiques concernant certains types de fraude. Toutefois, la société a indiqué que les niveaux de fraude qu'elle avait enregistrés en 2001 se situaient à des niveaux historiquement bas, comparés aux valeurs particulièrement élevés du début des années 1990.<sup>48</sup>

### **Statistiques sur la criminalité**

Dans certains pays, on dispose de données émanant des procédures judiciaires en relation avec la criminalité informatique. C'est notamment le cas de l'Allemagne.<sup>49</sup> Dans ce pays, les tribunaux produisent des statistiques basées sur les infractions pénales spécifiées dans le Code pénal allemand. Ce sont notamment les infractions commises en relation avec les TIC aux termes des articles relatifs à l'espionnage de données (article 202a), la fraude informatique (article 263a), la falsification de documents de preuve (article 269), l'altération de données (article 303a) et le sabotage informatique (article 303b). Cette typologie peut être conservée pour l'analyse des chiffres.<sup>50</sup> Selon cette typologie, 96 % de la criminalité en relation avec les TIC concernent essentiellement la fraude informatique aux termes de l'article 263a du Code pénal allemand. Le nombre des condamnations en vertu de cet article a augmenté de 71 %, passant de 1 531 en 1995 à 2 670 en 2002. Pour les autres catégories, on enregistre également de fortes progressions, mais à partir de chiffres initiaux beaucoup plus bas sur cette même période.

L'augmentation du nombre d'affaires enregistrée en Allemagne est incontestablement liée au développement de l'utilisation des TIC et à l'introduction de nouveaux services dans le pays. Les données fournies par l'enquête sur l'utilisation des TIC par les ménages aident à situer la progression de l'utilisation abusive des TIC dans les préoccupations globales des utilisateurs ou des utilisateurs potentiels. Pour les ménages qui ne sont pas en ligne, les données recueillies par l'Office statistique fédéral allemand indiquent que les facteurs économiques et ceux liés à la maîtrise de la technologie sont considérés comme des obstacles plus importants à l'utilisation d'Internet que la confiance et la sécurité.<sup>51</sup> Cela ne signifie pas nécessairement toutefois que les individus considèrent la sécurité et la confiance comme négligeables. Cela peut simplement indiquer que d'autres facteurs sont considérés comme des obstacles plus importants.

Outre la confiance et la sécurité, l'absence de maîtrise de la technologie et d'expérience pratique peut être aussi une source de préoccupation. Il ressort que l'enquête auprès des ménages non reliés à Internet que ceux-ci avancent le fait qu'ils n'en éprouvent pas le besoin (69 %) comme principale raison pour ne pas disposer d'une connexion Internet. Les autres raisons citées sont notamment le coût des équipements et de l'accès (33 % et 29 % respectivement) et le manque de maîtrise de la technologie (31 %). Les inquiétudes suscitées par la protection des données et la sécurité ne sont citées que par 12 % des ménages non raccordés comme la raison pour laquelle ils ne disposent pas d'une connexion Internet.

Les autorités chargées de l'application des lois aux États-Unis publient également des données sur leurs actions contre la cybercriminalité. L'opération Web Snare, lancée par le ministère de la Justice des États-Unis est un exemple d'une telle initiative.<sup>52</sup> L'opération Web Snare visait à réprimer tout un ensemble de délits économiques en ligne, notamment vol d'identité, fraude ou intrusion dans des systèmes informatiques ainsi que certains délits liés à la propriété intellectuelle. Plus de 160 procédures d'enquête ont été ouvertes dans le cadre de Web Snare, qui a fonctionné de juin à août 2004. Durant cette période, les enquêteurs ont identifié plus de 150 000 victimes, avec des pertes estimées à plus de USD 215 millions. Plus de 140 mandats de perquisition et de saisie ont été exécutés dans le cadre de cette opération, et les procureurs ont obtenu plus de 117 plaintes, demandes d'information et mises en examen. Les charges ainsi recueillies ont conduit à plus de 150 arrestations ou condamnations.

### **Criminalité liée au vol d'identité et cybercriminalité**

En Australie, l'*Australian Bureau of Statistics* (via la *National Crime Statistics Unit* – NCSU) et l'*Australian High Tech Crime Centre* (AHTCC) élaborent des définitions de la cybercriminalité.<sup>53</sup> Une des définitions de la cybercriminalité proposée dans ces travaux est la suivante : « *Un délit dans lequel un ordinateur ou autre dispositif électronique (similaire) est utilisé comme instrument pour rendre possible ou faciliter la perpétuation d'un délit, ou est la cible d'un délit* ». <sup>54</sup> Selon cette définition, l'expression « rendre possible » désigne les délits commis directement à l'encontre d'ordinateurs, qui n'existeraient pas sans l'utilisation de l'informatique. S'agissant des délits « facilités », la définition renvoie à des délits traditionnels facilités par l'utilisation des technologies de l'information. La NCSU cite comme information essentielle à recueillir, la nécessité d'estimer l'ampleur de la cybercriminalité en termes d'impacts économiques (notamment coûts des mesures de sécurité et des pertes de temps), de nombre d'incidents et de nombre de victimes. Elle préconise également une collaboration internationale pour l'élaboration de normes et de méthodologies de recueil de données pour les statistiques sur la cybercriminalité.

Il existe des définitions légales concernant la criminalité liée à l'identité (c'est-à-dire vol d'identité et fraude sur l'identité) dans un nombre croissant de pays de l'OCDE.<sup>55</sup> On dispose aussi de quelques données sur la criminalité liée à l'identité mais celles-ci sont très variables, quant à leurs ordres de grandeur par rapport à la taille des économies considérées, ce qui donne à penser qu'il existe des variations dans les définitions utilisées. La FTC, par exemple, a chiffré le coût du vol d'identité aux États-Unis, pour les consommateurs et les entreprises, aux environs de USD 50 milliards en 2003.<sup>56</sup> Au Royaume-Uni, le coût annuel du vol d'identité pour l'économie britannique a été chiffré à USD 2.5 milliards par an.<sup>57</sup> Les estimations varient aussi considérablement à l'intérieur des pays. En Australie, faute de statistiques faisant autorité sur le coût de la fraude à l'identité, les estimations varient de moins de USD 1 milliard (*Securities Industry Research Centre of Asia-Pacific*) à plus de USD 3 milliards par an (*Commonwealth Attorney-General's Department*).<sup>58</sup>

Il n'y a que très peu de données disponibles sur la proportion des pertes financières considérées comme relevant de la criminalité liée à l'identité qui soient imputables à la cybercriminalité. Aux États-Unis, la *Federal Deposit Insurance Corporation* (FDIC) indique que les pertes dues au « piratage de comptes » (par exemple utilisation d'informations obtenues par hameçonnage, logiciel espion, etc.) sont considérées comme une part relativement faible du coût global du vol d'identité.<sup>59</sup> Cela dit, la FDIC note

une réticence des institutions financières à publier leurs pertes, au motif que les problèmes de relations publiques que cela entraînerait pourraient aggraver leurs pertes financières. La FDIC cite également des études distinctes par Gartner, entreprise privée de recherche sur les technologies de l'information, et de l'*American Bankers Association*, qui classent l'Internet comme l'une des sources les plus importantes pour le vol d'identité. La FDIC attire également l'attention sur la menace que représente le vol d'identité comme facteur préjudiciable à la confiance dans le commerce électronique.

### **Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et autres initiatives des pays européens en matière de sécurité**

En Europe, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), nouvel organisme de l'Union européenne, a été créée en mars 2004 pour aider la communauté à assurer un niveau particulièrement élevé de sécurité des réseaux et de l'information et concourir à l'émergence de la « culture de sécurité » nécessaire, dans l'intérêt des citoyens, des consommateurs, des entreprises et des organismes du secteur public de l'Union européenne, au bon fonctionnement du marché intérieur.<sup>60</sup> Le mandat de l'ENISA prévoit également la collecte et l'analyse de données sur les incidents de sécurité en Europe et sur les risques émergents.<sup>61</sup> L'ENISA se propose de publier des rapports, des évaluations, des recommandations, des résultats d'études, des avis et d'autres documents d'intérêt public concernant le domaine d'activité de l'Agence.<sup>62</sup>

Les gouvernements d'un certain nombre de pays européens ont mis en place des sites Web pour accroître la sensibilisation à la sécurité des TIC. Aux Pays-Bas, le service d'alerte national se propose de donner aux particuliers et aux PME des informations à jour concernant les incidents liés à la sécurité.<sup>63</sup> A cet effet, le service d'alerte national diffuse des mises en garde et des alertes. Le service d'alerte national opère pour le compte du ministère des Affaires économiques et il est implanté au sein de la Computer Emergency Response Team du Gouvernement néerlandais. Au Royaume-Uni, « Itsafe » est un service gouvernemental chargé de donner tant aux particuliers qu'aux PME des conseils pour les aider à protéger les ordinateurs, les téléphones mobiles et autres équipements des attaques malveillantes ainsi que d'activités comme l'hameçonnage.<sup>64</sup> En Australie, l'*Australian High Tech Crime Centre* (AHTCC) remplit des fonctions analogues.<sup>65</sup> Le site Web de l'OCDE consacré à la culture de sécurité contient des liens vers des sites Web de ce type dans l'ensemble de la zone de l'OCDE.<sup>66</sup>

### **Exemples choisis de menaces/attaques/incidents sur Internet et disponibilité des données**

#### ***Hameçonnage et « pharming »***

L'hameçonnage est l'expression utilisée pour désigner l'utilisation de courriers électroniques et de sites Web frauduleux (« leurres ») conçus pour amener les internautes à révéler des informations personnelles. Les informations recherchées par les « hameçonneurs » sont notamment les numéros de cartes de crédit, numéros de compte, mots de passe, numéros d'identification personnelle, etc. Ces informations sont ensuite utilisées par les pirates pour conduire des activités frauduleuses tant en ligne qu'hors ligne.

La forme la plus courante d'hameçonnage consiste à adresser à un internaute un courrier électronique comportant une adresse « usurpée ». L'usurpation d'adresse désigne toute falsification d'un identificateur Internet telle qu'une adresse de courrier électronique, un nom de domaine ou une adresse IP. S'agissant du courrier électronique, l'entête est falsifiée pour masquer son origine et faire croire qu'il provient d'une autre source. Le « pharming » ou « empoisonnement du cache » est une technique basée sur le même type d'usurpation d'identificateur, mais qui utilise en outre des logiciels malveillants ou des logiciels espions pour rediriger les internautes souhaitant consulter des sites Web authentiques vers des sites frauduleux qui en reproduisent l'apparence (en général, par piratage ou empoisonnement du cache des serveurs DNS).<sup>67</sup>

L'usurpation d'identité pourrait également se développer en relation avec l'hameçonnage via la téléphonie sur Internet.<sup>68</sup>

Dans une attaque par hameçonnage, il s'agit généralement de remplacer le nom d'un tiers de confiance (par exemple, le nom d'une banque) par un autre. Ainsi, un internaute peut recevoir un courrier électronique émanant de [support@hameçon.com](mailto:support@hameçon.com) qui apparaîtra à l'Internaute comme un courrier émanant de [support@mabanque.com](mailto:support@mabanque.com). Le courrier d'hameçonnage tentera alors d'inciter l'internaute à utiliser un site Web qui peut lui-même imiter le site Web légitime de la banque.<sup>69</sup> L'internaute sera alors encouragé à divulguer des informations sensibles directement, ou, si son PC n'est pas protégé, à transférer à son insu des programmes malicieux qui par la suite généreront un transfert d'informations. Ainsi, des programmes appelés « chevaux de Troie » permettent d'enregistrer les noms d'utilisateurs et mots de passe de l'internaute quand celui-ci se reconnecte ensuite à un site légitime, par mémorisation des touches sur lesquelles il appuie.<sup>70</sup>

### *Statistiques sur l'hameçonnage*

L'ensemble le plus fiable de données sur l'hameçonnage est produit par l'*Anti-Phishing Working Group* (APWG).<sup>71</sup> L'APWG est une association professionnelle attachée à éliminer le vol d'identité et les activités frauduleuses induites par le problème croissant de l'hameçonnage et de la falsification de courrier électronique. L'APWG compte plus de 1 100 membres dont plus de 700 entreprises, 8 des 10 plus grosses banques des États-Unis, 4 des 5 principaux fournisseurs de services Internet aux États-Unis et plus de 100 constructeurs et éditeurs. L'APWG compte également parmi ses membres des organismes chargés de l'application des lois en Australie, au Canada, au Royaume-Uni et aux États-Unis.

L'APWG diffuse un large éventail de données sur différentes catégories telles que :

- Nombre d'attaques individuelles par hameçonnage signalées en décembre 2004 (1 707).
- Taux de progression annuel moyen des attaques par hameçonnage entre juillet et décembre 2004 (24 %).
- Pays hébergeant le plus de sites Web d'hameçonnage en décembre 2004 (annexe3, tableau 10).
- Nombre de marques victimes d'attaques par hameçonnage en décembre 2004 (55).
- Pourcentage d'attaques dans lesquelles l'URL contenait sous une forme ou une autre le nom de la cible (24 %).
- La durée de vie moyenne d'un site d'hameçonnage (5.9 jours).
- Une estimation selon laquelle 75 à 150 millions de courriers électroniques d'hameçonnage sont envoyés chaque jour sur l'Internet (grâce aux filtres antispam et à d'autres technologies, la majorité de ces messages ne parvient jamais jusqu'aux internautes).<sup>72</sup>

On pourrait disposer d'un volume croissant de chiffres sur les sites Web d'hameçonnage grâce à des outils conçus pour protéger contre les activités suspectes. Un certain nombre de FAI et de sociétés de sécurité, telles que Earthlink et GeoTrust, proposent désormais des barres d'outils qui identifient les sites d'hameçonnage (et les bloquent) ou authentifient les sites de confiance.<sup>73</sup> eBay a également lancé une barre d'outils gratuite pour ses acheteurs. Parmi les services proposés par la barre d'outils « Account Guard », figurent l'affichage d'alertes quand l'internaute se connecte à un site Web potentiellement frauduleux.<sup>74</sup> Par ailleurs, Microsoft a annoncé son intention d'intégrer des protections anti-hameçonnage dans les futures

versions d'Internet explorer.<sup>75</sup> Un point commun entre tous ces outils est qu'ils peuvent retourner à leurs auteurs des données sur leur utilisation et donc permettent l'échange de données non personnelles entre utilisateurs.

Netcraft, société de sécurité basée au Royaume-Uni, offre une barre d'outils gratuite qui donne des informations détaillées à ses utilisateurs et leur signale quand ils doivent faire preuve de vigilance. L'outil de Netcraft compare les informations issues de ses enquêtes permanentes sur Internet avec l'information connue concernant le site Web consulté. Ainsi, si un internaute se rend sur un site Web se faisant passer pour sa banque alors que le site en question est hébergé en un lieu suspect et qu'il n'est opérationnel que depuis deux jours, la barre d'outils le signalera à l'utilisateur. La barre d'outils de Netcraft commence également à générer des données sur l'hébergement de sites d'hameçonnage (ou de pharming) par pays (annexe 3 : tableau 11). Il est important de noter à propos des données tant de l'APWG que de Netcraft que les véritables auteurs de l'attaque par hameçonnage peuvent ne pas être situés dans le pays où le site Web est hébergé.

Les sites d'hameçonnage et de pharming n'utilisent pas tous des identificateurs Internet falsifiés. Il arrive que des internautes crédules soient redirigés non pas vers des adresses Internet falsifiées mais vers des sites Web au contenu trompeur. Ces sites « leurres » sont souvent utilisés pour certains types de fraude comme le « fake africain ou scam 419 ». En mars 2005, une base de données contenait plus de 3 000 sites actifs ou inactifs de fausses banques, etc., et de nouvelles entrées étaient ajoutées quotidiennement.<sup>76</sup> Bien que les noms de domaines, dans ces exemples, ne soient pas falsifiés, l'information donnée par les responsables des sites est invariablement fausse ou trompeuse.

Il arrive aussi que des données sur l'hameçonnage soient obtenues indirectement, à l'occasion de la mesure d'un autre phénomène. Brightmail, société acquise par Symantec en juin 2004, mesure le volume de spams filtrés par son logiciel et reçus par plusieurs millions de ses comptes factices. Elle a fait savoir au début de 2004 que son logiciel était utilisé pour filtrer plus de 80 milliards de messages chaque mois, soit l'équivalent de 15 % de l'ensemble du courrier électronique sur Internet à l'échelle mondiale. Actuellement, selon Brightmail, environ 5 % de l'ensemble du spam qu'elle traite sont liés à des attaques par hameçonnage. Elle constate que l'hameçonnage a progressé à l'échelle mondiale, passant de 300 millions de messages en août 2003 à plus de 2.9 milliards de messages en mars 2004.

#### *Le coût de l'hameçonnage*

Les estimations du coût de l'hameçonnage varient de façon considérable. À une extrémité, certaines institutions financières, bien que ne voulant pas révéler leurs propres pertes financières, indiquent que les sommes sont relativement modestes. L'*Association for Payment Clearing Services* (APACS) du Royaume-Uni est une association non statutaire d'institutions assurant des services de paiement pour leur clientèle. En mars 2005, l'APACS a chiffré le coût de la fraude bancaire en ligne (du fait essentiellement d'attaques par hameçonnage) parmi ses membres au Royaume-Uni à USD 25 millions pour 2004.<sup>77</sup> C'était la première fois que l'APACS recueillait des données sur l'hameçonnage.

Une étude réalisée par le *Ponemon Institute* et parrainée par la NACHA (Association de sociétés de paiement électronique basée aux États-Unis) et TRUSTe, organisme sans but lucratif pour la protection de la vie privée en ligne, a révélé que 76 % des consommateurs aux États-Unis étaient victimes d'un nombre croissant d'incidents de falsification d'identité et d'hameçonnage et que 35 % recevaient des courriers électroniques malicieux au moins une fois par semaine.<sup>78</sup> Le rapport, en septembre 2004, estimait que les pertes financières totales pour les victimes de ces incidents s'élevaient approximativement à USD 500 millions aux États-Unis.

Gartner a également tenté de chiffrer le coût de l'hameçonnage aux États-Unis. Les résultats de Gartner semblent indiquer que le problème a davantage d'ampleur. Dans une étude publiée en mai 2004, Gartner a estimé que les pertes directes du fait de la fraude par falsification d'identité des victimes d'attaques par hameçonnage aux États-Unis avaient coûté aux banques et aux sociétés de délivrance de cartes de crédit quelque USD 1.2 milliard durant l'année 2003.<sup>79</sup>

D'autres études couvrant une zone géographique plus vaste donnent des résultats différents concernant les pertes dues à l'hameçonnage. Selon le TowerGroup, les pertes mondiales imputables à l'hameçonnage par courrier électronique ont été de l'ordre de USD 137 millions en 2004.<sup>80</sup> Le TowerGroup déclare que le nombre effectif d'attaques par hameçonnage s'est élevé au total à plus de 31 000 à l'échelle mondiale en 2004 et que selon ses estimations, le chiffre pourrait dépasser 86 000 en 2005.

On peut donc se demander pourquoi les estimations des pertes directes imputées aux victimes d'hameçonnage varient dans de telles proportions. Cela peut être dû en partie au fait que les institutions financières, tout en prenant la menace au sérieux, hésitent à révéler publiquement leurs pertes. Par ailleurs, il se peut que certaines entreprises ignorent tout simplement l'ampleur des pertes si celles-ci ne sont pas signalées par leurs clients. Globalement, du fait de ces facteurs, il serait très difficile pour l'industrie de déterminer un chiffre définitif pour les pertes financières directes imputables à l'hameçonnage.

L'APWG signale qu'en détournant des marques de confiance de banques, détaillants et de sociétés de cartes de crédit bien connus, les pirates pratiquant l'hameçonnage parviennent à tromper 5 % des destinataires de courriers électroniques falsifiés. Au Royaume-Uni, l'APACS a fait réaliser des recherches qui ont montré que 4 % des utilisateurs de services bancaires par Internet répondraient à un courrier électronique, censé provenir de leur banque, leur demandant de cliquer sur un lien pour saisir de nouveau leurs informations confidentielles.<sup>81</sup> Sur la base de données d'enquêtes, Gartner estime qu'environ 19 % des personnes attaquées, soit près de 11 millions d'internautes adultes aux États-Unis, ont cliqué sur le lien d'un courrier électronique contrefait pour hameçonnage.<sup>82</sup> Gartner signale en outre que 3 % des personnes attaquées, soit selon les estimations 1.78 million d'adultes aux États-Unis, auraient communiqué à des pirates leurs informations financières ou personnelles en 2003.

L'étude du *Ponemon Institute*, qui repose sur un échantillon national de 1 335 internautes sur l'ensemble du territoire des États-Unis, a montré que 7 déclarants sur 10 avaient visité de manière fortuite un site Web falsifié.<sup>83</sup> L'étude signalait en outre que plus de 15 % des déclarants piratés admettaient avoir été « hameçonnés », dans la mesure où ils avaient communiqué des informations privées. Au total, l'étude a montré qu'un peu moins de 2 % de l'ensemble des déclarants pensaient avoir subi un préjudice financier direct du fait de l'attaque par hameçonnage.

Dans l'étude 2005 « State of the Net » de *Consumer Reports*, les auteurs indiquent que l'incidence globale de l'hameçonnage était faible mais en augmentation rapide, un déclarant sur 200 subissant des pertes. *Consumer Reports* indiquait en outre que le coût moyen par incident était de USD 395, soit un total de USD 147 millions de pertes pour les États-Unis.

#### *Statistiques concernant la falsification d'identité*

Un projet expérimental est en cours par l'*Advanced Network Architecture Group* (ANA) au MIT pour tenter de mesurer de façon globale le filtrage et l'usurpation d'adresses IP sur Internet. Bien que les données de l'ANA du MIT soient considérées comme les plus complètes de ce type, le projet est toujours en cours de développement. Les données rendues disponibles ne sont représentatives que des blocs d'adresses IP et systèmes autonomes des réseaux volontaires dont l'ANA a reçu les rapports. C'est la raison pour laquelle l'ANA présente des données sur la base à la fois de ses observations et de ses

estimations globales des identificateurs Internet « falsifiables ». L'ANA travaille également à corrélérer ces données avec les implantations géographiques, les premiers résultats devant être communiqués en 2005.

Un autre domaine à l'étude, lié à l'adressage et aux identificateurs sur Internet, est l'attaque par empoisonnement du cache dans le système de noms de domaine (DNS).<sup>84</sup> En mars et avril 2005, le *SANS Internet Storm Center* a signalé un certain nombre d'attaques de ce type. Il s'agit en l'occurrence d'attaques qui reconfigurent les serveurs de noms racines pour qu'ils donnent un nom falsifié. Cette information est ensuite conservée dans le cache et les demandes suivantes de noms, dans la zone « empoisonnée » sont redirigées vers le serveur de nom piraté qui, à son tour, fournit des informations falsifiées. La *Measurements Factory* élabore une procédure automatique de balayage pour détecter les cas d'empoisonnement du cache des serveurs DNS et elle se propose de publier toutes les semaines des statistiques à l'intention des membres du *DNS Operations, Analysis, and Research Center* (DNS-OARC) et des opérateurs de réseaux.<sup>85</sup>

### **Logiciels espions**

Une catégorie de logiciels qui pourraient avoir de graves implications pour la sécurité et la confiance est ce que l'on désigne par le terme générique de « logiciels espions ». La *Federal Trade Commission* définit concrètement les logiciels espions comme « des logiciels qui aident à recueillir des informations sur une personne ou une organisation à leur insu et qui peuvent envoyer ces informations à une autre entité sans le consentement du consommateur, ou prendre le contrôle d'un ordinateur sans le consentement du consommateur ».<sup>86</sup> La FTC considère que bien que celle-ci constitue un point de départ utile, elle souhaiterait voir un consensus plus large au sein de l'industrie sur la définition des logiciels espions et la divulgation d'informations aux consommateurs.<sup>87</sup>

Une initiative dans ce sens a été prise par l'*Anti-Spyware Coalition* (ASC), groupe composé de sociétés de logiciels anti-espions, d'universitaires et de groupes de défense des consommateurs.<sup>88</sup> En août 2005, l'ASC a diffusé un document de consultation proposant une typologie des logiciels espions et autres logiciels similaires.<sup>89</sup> Ce document contenait également un glossaire définissant les termes utilisés dans les discussions sur les logiciels espions. PTS, l'autorité de régulation des communications en Suède, a également réalisé un rapport sur les logiciels espions et autres phénomènes de même type. Le rapport aborde les questions de définition et d'identification de ce qui différencie les logiciels espions des phénomènes apparentés comme les virus.<sup>90</sup>

Alors qu'un virus s'efforcera de nuire au système d'un utilisateur ou d'utiliser ce système pour nuire à autrui, le logiciel espion vise à surveiller l'utilisation du système (par exemple, succession des touches frappées au clavier, ou pages Web visitées) ou à extraire des informations contenues dans le système (par exemple, analyse du disque dur). Comme pour l'hameçonnage, l'information recherchée peut être des numéros de cartes de crédit, des noms de comptes, des mots de passe, des numéros d'identification personnelle, etc. Cette information est ensuite transmise à l'auteur de l'attaque par logiciel espion.

Le logiciel espion couvre une catégorie plus vaste que l'hameçonnage, même si certaines des techniques utilisées sont identiques. Une distinction majeure est que l'hameçonnage a presque systématiquement une intention criminelle. Le logiciel espion peut, bien entendu, être lui aussi utilisé pour des fraudes ou vols d'identité. Mais certaines applications de logiciels espions peuvent être classées dans la catégorie des logiciels qui sont une source d'irritation pour les utilisateurs, qui sont perçus comme intrusifs par les utilisateurs ou qui nuisent aux performances du système (par exemple utilisation non autorisée de la bande passante d'un utilisateur, plantage ou instabilité du système). Une expérimentation effectuée avec des machines infectées a montré que 8 % du trafic sortant était dû à des logiciels espions.<sup>91</sup> Des logiciels espions peuvent également être utilisés pour sonder un système de manière à trouver une porte d'entrée qui pourrait être exploitée par des pirates.<sup>92</sup>

### *Statistiques sur les logiciels espions*

Dans son discours liminaire lors d'un séminaire de la FTC sur les logiciels espions en avril 2004, le *Director of the Bureau of Consumer Protection*, Howard Beales notait : « Comme les logiciels espions sont un phénomène nouveau, il n'y a eu que peu de recherches empiriques et d'analyses pour évaluer leur prévalence et leurs effets d'une façon relativement systématique. Mais les anecdotes abondent. Et les éléments disponibles donnent à penser que les consommateurs sont préoccupés par les logiciels espions et par ce que ceux-ci peuvent provoquer. Les consommateurs ont ainsi téléchargé plus de 45 millions de fois des versions gratuites des deux programmes anti-logiciels espions les plus largement utilisés et de nombreux fournisseurs d'accès à Internet ont commencé à offrir des moyens de détection de logiciels espions pour répondre aux inquiétudes des consommateurs à l'égard de ces logiciels ». <sup>93</sup>

On dispose de tout un ensemble de données provenant de sources industrielles sur les logiciels espions. Les plus courantes sont celles dérivées des programmes destinés à prévenir le téléchargement de logiciels espions par l'utilisateur ou à supprimer les logiciels espions présents sur le système d'un utilisateur. Selon l'une de ces sources, il existe plus de 100 logiciels d'analyse anti-spyware disponibles en téléchargement. <sup>94</sup> L'une des plus importantes de ces bases de données est tenue à jour par PestPatrol, qui appartient à *Computer Associates International*. PestPatrol définit les logiciels malicieux comme « tout logiciel non sollicité ». PestPatrol a également publié un glossaire détaillé des différentes sous-catégories. <sup>95</sup> Sur la base de ces définitions, PestPatrol rend disponible tout un ensemble d'indicateurs dérivés de ses activités (annexe 3, figures 8, 9, 10 et 11). <sup>96</sup> McAfee publie également un ensemble détaillé de statistiques obtenues par le recueil anonyme de données auprès des utilisateurs de ses produits. <sup>97</sup>

En août 2003, McAfee détectait moins de 2 millions de « adware » ou logiciels espions. Mais en mars 2004, le nombre total avait progressé jusqu'à dépasser 14 millions. <sup>98</sup> Pour prendre un autre exemple, Earthlink est un FAI qui met un logiciel anti-logiciel espion à la disposition de ses utilisateurs et publie des statistiques. <sup>99</sup> Les données d'Earthlink font également apparaître une forte progression dans le temps du volume de logiciels espions détectés. Le rapport semestriel de Symantec propose une analyse et une discussion des tendances concernant les attaques sur Internet, notamment en ce qui concerne les codes malveillants créés pour pirater des informations confidentielles. <sup>100</sup> Le rapport pour la période allant de juillet à décembre 2004 met en évidence une forte progression de ce phénomène.

En 2005, Microsoft a diffusé une version bêta d'un nouveau programme anti-logiciel espion et l'a mise gratuitement à la disposition des utilisateurs de Windows. Le logiciel permet aux utilisateurs de transmettre anonymement des informations à Microsoft et, en février 2005, la société recevait plus d'un demi million de rapports par jour. <sup>101</sup>

### *Le coût des logiciels espions*

Certains spécialistes de la sécurité mettent en garde contre le fait que les logiciels espions obligent déjà certaines institutions financières à réduire l'éventail des services qu'elles offrent à leurs utilisateurs, et sapent la confiance dans le commerce électronique. <sup>102</sup> Dans le même temps, on ne dispose que de peu de données qui permettraient d'estimer le coût des logiciels espions, en proportion du total des pertes dues au vol d'identité, pour les entreprises et les consommateurs. On dispose toutefois de certains indicateurs indirects. En 2004, McAfee a signalé que les logiciels espions devenaient un problème de soutien technique plus significatif que les virus en termes d'appel à ses services d'assistance. L'expérience des autres sociétés semble confirmer que globalement les logiciels espions et les virus sont ceux qui provoquent les plus fortes pertes et préoccupent le plus les utilisateurs.

Selon Dell, premier fournisseur mondial d'ordinateurs personnels, « ... le nombre record de clients contactant Dell avec des problèmes de performances de leur ordinateur imputables à des logiciels espions

ou des virus montre l'ampleur prise par le problème parmi les particuliers utilisateurs d'équipements technologiques. Jusqu'à 20 % des appels reçus par les équipes de soutien technique d'ordinateurs grand public de Dell portent sur des problèmes de logiciels espions et de virus, loin devant n'importe quel autre problème de performance ». <sup>103</sup> Un participant à l'atelier de la FTC a rapporté que la durée moyenne d'un appel au service d'assistance d'un FAI est de 6 minutes, alors que dans le cas d'un appel portant sur un problème de logiciel espion, elle atteint 25 minutes. <sup>104</sup> Dans le même temps, selon Microsoft, plus d'un tiers des utilisateurs signalant des plantages de leurs applications sont confrontés en fait à des problèmes de logiciel espion. <sup>105</sup> De telles occurrences génèrent des coûts pour les entreprises et les consommateurs, en même temps qu'elles sapent la confiance qu'ont les consommateurs à l'égard des fournisseurs de matériel et de services auxquels ils sont susceptibles d'imputer les problèmes générés par les logiciels espions.

En mars 2005, il a été signalé que la police britannique avait fait échouer une tentative d'utilisation d'un logiciel espion contre d'une banque, pour faire effectuer un transfert illégal de USD 423 millions. <sup>106</sup> Dans cette affaire, les pirates avaient utilisé un logiciel d'enregistrement des touches qui leur permettait de suivre les saisies effectuées en interne sur les claviers des ordinateurs. Que des criminels arrivent à recueillir de l'argent grâce aux logiciels espions semble confirmé par le fait que ceux-ci font également des offres non sollicitées à des développeurs de logiciels. En février 2005, l'*Internet Storm Center* a fait état d'offres dans lesquelles le développeur d'un programme (par exemple, un jeu) intégrant trois modules de logiciels espions aurait reçu USD 0.25 pour chaque installation du logiciel. <sup>107</sup>

Avec l'extension du marché de la publicité sur Internet, le marché gris des logiciels espions et « adware » semblent avoir acquis un nouvel attrait. Webroot, qui est un éditeur de programmes d'élimination de logiciels espions, évalue le retour moyen d'une installation d'un logiciel espion à USD 2.40 par an. <sup>108</sup> Ces recettes viennent des sommes perçues pour afficher des fenêtres publicitaires, rediriger les utilisateurs vers des pages Web, etc. Selon des estimations de Webroot, les trois programmes de cette catégorie qui ont la plus forte base installée à l'échelle mondiale pourraient générer près d'un demi-milliard de dollars par an.

Des économistes ont également commencé à explorer les retours sur investissements dans la sécurité comparés à diverses formes d'attaque sur Internet, depuis le spam jusqu'au logiciel espion, dans l'optique de l'attaquant. <sup>109</sup> Bien que ces travaux débouchent sur des modèles économétriques qui peuvent être employés pour ce type d'analyse, ils ont tendance à être limités par le manque de disponibilité de données.

Dans son rapport 2005 sur l'état du Net, *Consumer Reports* indique que l'incidence globale des logiciels espions se caractérisait par une croissance explosive, une personne interrogée sur six ayant connu un problème majeur, souvent coûteux. *Consumer Reports* indique en outre que le coût moyen par incident pour les consommateurs a été de USD 250, soit un total national de USD 3.5 milliards de pertes aux États-Unis.

### ***Virus, vers, chevaux de Troie et autres incidents***

De nombreuses organisations et sociétés rendent publiques des informations sur leurs activités de sécurité à l'égard des réseaux informatiques. McAfee, par exemple, publie des statistiques sur ses activités à l'échelle mondiale. Parmi celles-ci figure notamment une carte du monde indiquant l'ampleur de l'activité virale par pays. <sup>110</sup> Les données de McAfee, sur les virus les plus fréquents, sont également ventilés par région. Le site Web de Symantec donne un synopsis des menaces virales les plus récentes découvertes par *Symantec Security Response*, et précise notamment : le classement par catégorie (risque), le nom de la menace (menace), le jour auquel la menace a été identifiée (découverte) et le jour auquel une définition virale a été ajoutée pour protéger contre la menace (protection). <sup>111</sup>

Des données similaires sont également disponibles auprès de sources qui n'ont pas de lien avec des fournisseurs. Depuis novembre 2000, DSshield propose une plate-forme permettant aux utilisateurs de pare-feu d'échanger des informations sur les cas d'intrusion.<sup>112</sup> DSshield est un service gratuit qui bien que créé au départ sur une base volontaire bénéficie maintenant du soutien du SANS Institute. En regroupant les informations de nombreux utilisateurs, qui téléchargent des applications rendant compte de l'activité des pare-feu, DSshield permet de réunir des informations géographiques sur les attaques et les tendances en matière d'incidents.<sup>113</sup> Ces mêmes données sont disponibles auprès de l'*Internet Storm Center* exploité par le SANS.<sup>114</sup> Un indicateur que le SANS rend public à partir des données recueillies est « la durée de survie » mensuelle. Cette « durée de survie » est la durée moyenne entre deux tentatives d'intrusion (par vers, par exemple) notifiées par les pare-feu des utilisateurs participants.<sup>115</sup>

Le *National Institute of Standards and Technology* (NIST) est un organisme fédéral sans pouvoir réglementaire au sein de la *Technology Administration* du ministère du Commerce des Etats-Unis.<sup>116</sup> La mission du NIST est d'élaborer et promouvoir des méthodes de mesure, des normes et des technologies destinées à améliorer la productivité, faciliter les échanges et améliorer la qualité de la vie. La *Computer Security Division* du NIST tient à jour un index consultable des vulnérabilités informatiques (ICAT Metabase). L'ICAT renvoie les utilisateurs vers tout un ensemble de bases de données sur les vulnérabilités et de sites de mises à jour disponibles publiquement, ce qui permet aux utilisateurs d'identifier et de corriger les vulnérabilités existant sur le système. L'ICAT n'est pas en elle-même une base de données sur les vulnérabilités, mais plutôt un index consultable permettant d'orienter l'utilisateur vers des sources sur les vulnérabilités et les informations permettant d'y remédier. L'ICAT propose toutefois des statistiques sur les vulnérabilités, notamment selon une présentation chronologique.<sup>117</sup> Le *Cassandra Tool* du CERIAS, à l'université Purdue, est un site dont l'objet est d'aider les utilisateurs à se tenir informés des statistiques de la base de données ICAT.<sup>118</sup>

Les *Computer Emergency Readiness Teams* (CERT) dont le nombre augmente constamment partout dans le monde sont autre source de données sur les menaces et vulnérabilités dans ce domaine. À l'échelle mondiale, on dénombre plus de 250 organisations utilisant la dénomination « CERT » ou une appellation similaire, chargées de faire face aux menaces sur la cybersécurité.<sup>119</sup> L'US-CERT, par exemple, est un partenariat entre le *Department of Homeland Security* et les secteurs public et privé. On peut également citer comme autre exemple du secteur soit public soit privé AUSCERT (Australie), CanCERT (Canada), CERT-IST (France), JPCERT (Japon), KrCERT (Corée) et APCERT (*Asia Pacific Computer Emergency Response Team*) qui est une coalition de CSIRT (*Computer Security Incident Response Teams*), de 12 économies de toute la région Asie-Pacifique.<sup>120</sup>

Un certain nombre de CERT diffusent des statistiques sur leurs activités. L'US-CERT propose des statistiques sur les incidents dans des domaines comme les attaques par déni de services, l'utilisation de codes malveillants, etc.<sup>121</sup> Le CERT japonais diffuse des rapports établis à partir d'un réseau de points d'observation répartis qui détectent les infections par vers et sondent les systèmes vulnérables.<sup>122</sup> Les données sont utilisées pour l'organisation des activités du JPCERT concernant la publication d'alertes et d'avis et l'organisation de programmes de sensibilisation à la sécurité. Le CERT coréen publie également un large éventail de statistiques sur les incidents.<sup>123</sup>

Dans son rapport 2004, *Global Security Index Report*, publié en février 2005, IBM mentionne les téléphones mobiles cellulaires et les assistants numériques comme un nouveau vecteur de diffusion de virus, spams et autres menaces potentielles sur la sécurité.<sup>124</sup> En 2004, le premier « ver » s'attaquant à la téléphonie mobile est apparu. Le ver dit « Cabir » se diffuse par Bluetooth.<sup>125</sup> En février 2005, selon F-Secure, qui est une société finlandaise de sécurité, le virus Cabir s'était répandu dans 14 pays.<sup>126</sup> Le même mois, un certain nombre d'invasions spectaculaires de la vie privée ont été observées via les téléphones mobiles cellulaires.<sup>127</sup> En mars 2005, F-Secure a annoncé qu'ils avaient trouvé le premier virus

capable de se diffuser via les services MMS (*multimedia messaging services*) dont les messages peuvent contenir des photos, des sons ou des vidéos, sur téléphone mobile.<sup>128</sup>

CAIDA, (*Cooperative Association for Internet Data Analysis*) propose des outils et analyses destinés à faciliter l'organisation et la maintenance d'une infrastructure Internet mondiale robuste et modulaire. CAIDA est hébergée par le *San Diego Supercomputing Center* (SDSC), qui est une extension de l'université de Californie à San Diego (UCSD).<sup>129</sup> Parmi les outils développés par CAIDA, un certain nombre facilitent les investigations liées à la sécurité et la gestion des réseaux. Les travaux de CAIDA dans ce domaine consistent notamment à recueillir des données et à analyser des attaques par déni de services, par vers se propageant sur Internet, par pollution des serveurs racines, etc. La recherche menée vise notamment à élaborer des outils permettant la visualisation de phénomènes comme l'infection des machines raccordées à Internet.<sup>130</sup>

### *Le coût des virus et des vers*

Il n'existe pas de chiffres faisant autorité sur le coût économique des virus informatiques, vers, chevaux de Troie, etc. Un certain nombre de sources produisent des estimations des coûts pour les entreprises et les consommateurs pour des cas d'attaques isolées. Ces chiffres sont largement cités dans la presse, mais pas toujours sans un certain scepticisme quant à la méthodologie et aux résultats.<sup>131</sup> Pour la plupart, les méthodologies utilisées pour obtenir ces chiffres ne sont pas rendus publiques. Un autre point évoqué par les critiques de ces données est que lorsqu'elles sont produites par des entreprises de sécurité ou par des personnes travaillant pour ce type d'entreprise, elles ne sont pas considérées comme des sources indépendantes ou impartiales. Néanmoins, le coût de certaines attaques est sans doute significatif, même s'il n'est pas facilement quantifiable. Le SANS Institute, par exemple, a estimé pour deux vers informatiques les coûts de décontamination à plus de USD 1 milliard chacun en 2003.<sup>132</sup> Pour la même année, *Trend Micro*, société réputée de sécurité, a estimé le coût global des virus à USD 55 milliards, contre USD 30 milliards en 2002.<sup>133</sup> Prevx, société de sécurité logicielle, évalue le coût total des dix vers les plus destructeurs, pour l'année 2004, à USD 17.2 milliards.<sup>134</sup> Un certain nombre d'autres sources évaluent les coûts mondiaux à des niveaux encore plus élevés que ceux mentionnés, mais les résultats ainsi obtenus, et ceux cités ci-dessus, ne sont pas vérifiables.

Dans l'enquête CSI/FBI aux États-Unis, et l'enquête AusCERT en Australie, il est demandé d'indiquer les pertes provoquées par les virus, vers et chevaux de Troie. Pour cette catégorie, dans les enquêtes 2004, les déclarants ont signalé des pertes de l'ordre de USD 55 millions (États-Unis) et USD 5.6 millions (Australie). Bien que ces deux enquêtes comportent parmi les entreprises interrogées un échantillon de grandes entreprises, d'établissements d'enseignement et d'administration dans leur pays respectif, elles ne reflètent pas, bien entendu, les coûts pour l'ensemble de l'économie. Elles aident toutefois à mieux situer certaines estimations des coûts des virus appartenant au haut de l'échelle.

Dans le rapport 2005 sur l'état du Net de *Consumer Reports*, les auteurs indiquent que l'incidence globale des virus augmente, que ceux-ci ciblent davantage les informations confidentielles et qu'un déclarant sur quatre a connu un problème majeur, souvent coûteux. *Consumer Reports* indique en outre que le coût moyen par incident a été de USD 312 pour les consommateurs, soit un total national de USD 5.5 milliards de perte aux États-Unis.

### ***Botnets (machines zombies)***

Les « Botnets » sont un terme désignant des machines raccordées à l'Internet qui ont été compromises de telle manière qu'elles peuvent être commandées par un internaute de l'extérieur pour agir de concert, à l'insu du propriétaire ou contre sa volonté. Les botnets peuvent être utilisés par le pirate qui a pris le

contrôle des machines pour lancer des attaques par déni de service contre certains sites sur Internet ou pour retransmettre des spams, des messages d'hameçonnage, etc.

Les données disponibles sur les botnets proviennent principalement d'entreprises de sécurité ou d'organisations qui surveillent et combattent le phénomène. Le projet Honeynet (« réseau pot de miel ») par exemple, est une organisation de recherche sans but lucratif associant des professionnels de la sécurité qui déploient des systèmes, des applications et des services pour piéger des attaquants dans le monde entier. L'idée est de mieux connaître les outils et comportements des attaquants et de diffuser cette information auprès des spécialistes de la sécurité. En mars 2005, le projet Honeynet allemand a publié une étude détaillée des botnets.<sup>135</sup> Certains botnets surveillés par le projet Honeynet comprenaient jusqu'à 50 000 machines. L'étude détaille également la façon dont l'information est échangée par les pirates contrôlant les botnets, certaines de leurs caractéristiques (par exemple niveaux de maîtrise) et buts poursuivis, ainsi que des cas d'attaquants s'appropriant les machines déjà piratées par d'autres attaquants. L'US CERT a également proposé la création d'un programme de suivi des botnets qui, tout en constituant un outil permettant d'identifier et de répondre à ces menaces, permettrait aussi de recueillir et d'archiver des informations statistiques.<sup>136</sup>

Le « ZombieMeter » de CipherTrust suit à l'échelle mondiale l'activité des botnets, pour ce qui concerne la messagerie, en temps réel.<sup>137</sup> CipherTrust surveille l'activité sur les messageries grâce aux données reçues par le réseau des équipements de la société qui protègent les systèmes de messagerie de ses clients partout dans le monde. Le « ZombieMeter » permet aux visiteurs du site Web de CipherTrust de s'informer de l'activité des botnets en relation avec l'émission de messages et du nombre de machines infectées par pays.

Le nombre moyen d'ordinateurs que Symantec a détectés durant ses sondages quotidiens de botnets au premier semestre 2004 est passé de 2 000 à 30 000. Parfois, le nombre de machines infectées surveillées par Symantec a atteint 75 000.<sup>138</sup> Chaque botnet peut comprendre plusieurs milliers de machines. En 2004, par exemple, l'*Internet Storm Centre* a indiqué que Telenor, opérateur norvégien de télécommunications, avait démantelé un botnet composé de 10 000 machines piratées.<sup>139</sup> Pour le premier semestre 2004, Symantec a indiqué qu'il était fréquent d'observer des attaques pouvant regrouper jusqu'à 30 000 machines.<sup>140</sup> Pour le second semestre 2004, Symantec a fait état d'une réduction de la taille des botnets, qui s'explique peut être par la diffusion du Service Pack 2 de Windows XP.

Le rapport de Symantec « Internet Security Report Threat Report » pour le second semestre de 2004 contenait un nouvel indicateur sur les botnets, à savoir le pourcentage d'ordinateurs « zombies » par pays (annexe 3, tableau 12).<sup>141</sup> Symantec notait qu'en montrant la répartition mondiale des ordinateurs infectés, cet indicateur pouvait aider à mieux comprendre le niveau de sensibilisation à la sécurité des internautes dans un pays donné. Les résultats montraient que les pays où les ordinateurs infectés sont les plus nombreux sont le Royaume-Uni (25.2 %), les États-Unis (24.6 %) et la Chine (7.8 %). En pondérant les données sur les ordinateurs infectés par la population ou le nombre d'abonnés au haut débit, on peut obtenir également des informations utiles sur l'ensemble des pays de l'OCDE (annexe 3, tableau 13). Pour le premier indicateur comme pour le second, c'est au Royaume-Uni que le taux d'infection est le plus élevé. Si l'on fait abstraction de ce pays, par habitant, ce sont le Portugal, la Suède, le Canada et le Danemark qui comptent le plus grand nombre d'ordinateurs zombies. Par rapport au nombre total de leurs abonnés au haut débit, le Portugal, la Grèce, l'Espagne et la Suède sont les pays où le nombre d'ordinateurs zombies est le plus élevé, après le Royaume-Uni. Cela n'est bien entendu qu'un indicateur partiel dans la mesure où le nombre des abonnés par liaison commutée dont les ordinateurs sont également infectés n'est pas pris en compte. Des analyses plus poussées doivent être entreprises quant à l'impact que les connexions par liaison commutée pourraient avoir sur ces données, mais il est généralement admis que la multiplication des botnets a coïncidé avec l'essor de l'accès haut débit à Internet.

Symantec a laissé entendre que la proportion élevée observée au Royaume-Uni pouvait s'expliquer par la progression rapide du haut débit dans ce pays. Bien que ce soit incontestablement un facteur, on peut se demander pourquoi d'autres pays comme la France où les taux de pénétration – et de progression – du haut débit sont analogues à ce que l'on observe au Royaume-Uni, enregistrent une proportion beaucoup plus faible d'ordinateurs zombies.

L'explication la plus vraisemblable de cette disparité dans les taux d'infection réside sans doute dans la culture de sécurité qui prévaut selon les pays. Dans certains pays, les FAI fournissent à leurs clients, dans le cadre de leur abonnement, des moyens de sécurité. En Finlande, par exemple, tous les FAI fournissent à leurs clients des pare-feu personnels et des logiciels antivirus soit gratuits, soit à des prix très fortement réduits. Cela pourrait expliquer pourquoi la Finlande est le pays qui obtient le meilleur résultat parmi les pays nordiques quant au nombre d'ordinateurs zombies rapporté au nombre d'abonnés à haut débit. Le fait que d'autres pays, ailleurs dans la zone de l'OCDE, enregistrent des résultats encore meilleurs que la Finlande donne à penser que d'autres facteurs, outre la culture de sécurité en vigueur dans le pays, entrent également en jeu. Le plus important de ces facteurs est sans doute la sensibilisation et la réactivité des utilisateurs à la sécurité, pour la mise en oeuvre d'outils tels que pare-feu et logiciels antivirus, même lorsque ceux-ci sont fournis par les FAI. A cet égard, il convient de relever les taux d'infection très bas au Japon, en Belgique, en Corée et aux Pays-Bas. Dans tous ces pays, les taux de pénétration du haut débit sont très élevés et les taux d'infection faibles, ce qui tendrait à indiquer une utilisation relativement développée des pare-feu et logiciels antivirus par les internautes.

Symantec recueille des données sur les ordinateurs infectés grâce à 20 000 systèmes de détection implantés sur les réseaux de plus de 180 pays. Les attaques émanant d'ordinateurs infectés sont enregistrées et rapprochées avec les informations d'autres bases de données sur par exemple les codes malveillants ou celles permettant de déterminer les adresses d'origine. Il est significatif de noter que les données ne concernent pas uniquement les clients Symantec, afin que certains indicateurs ne soient pas biaisés sur le plan géographique. La prise de contrôle d'ordinateurs est considérée davantage comme une activité opportuniste que visant un pays donné en vue d'une utilisation à l'intérieur de ce pays. En conséquence, cet indicateur est peut-être l'un des meilleurs actuellement disponibles pour les comparaisons internationales de la sensibilisation à la sécurité et des mesures prises en la matière par les internautes.

#### *Le coût des botnets*

En 2004, un certain nombre de cas d'extorsion ont été signalés dans lesquels des propriétaires de sites Web de commerce électronique ont été menacés d'attaques par déni de service. Les sites Web de jeux en ligne étaient l'une des principales cibles, mais aussi des entreprises faisant intervenir des transactions financières sur le Web.<sup>142</sup> Ainsi, la *National Hi-Tech Crime Unit* a signalé que des pirates s'étaient attaqués au site Web d'un bookmaker en ligne au Royaume-Uni au moyen d'une attaque par déni de service. Les pirates ont fait savoir au bookmaker que leur attaque cesserait si le bookmaker transférait USD 40 000 sur un compte dans une banque lettone.<sup>143</sup> L'entreprise du bookmaker a accepté et transféré de l'argent à plusieurs reprises, mais quand les attaques se sont poursuivies, elle a contacté la *National Hi-Tech Crime Unit*. Il ressort des poursuites engagées contre les auteurs présumés, en Russie, que les pertes totales subies par les victimes de ce seul gang ont été chiffrées à USD 3 millions. Cela correspond à une estimation du manque à gagner et des versements effectués aux auteurs présumés de l'extorsion de fonds. Les pertes seraient sans doute difficiles à chiffrer dans de nombreux cas. Des études universitaires récentes donnent à penser que lorsque des sites Web deviennent indisponibles à la suite d'attaques par déni de service, cela a un effet négatif durable.<sup>144</sup> Il ressort de ces travaux que les sites pour lesquels l'internaute peut à moindre coût s'adresser ailleurs sont les plus durement touchés par ces attaques.

En 2004, des sociétés bien connues comme Akamai et Doubleclick ont également été victimes d'attaques par déni de service.<sup>145</sup> Dans un cas dont on a beaucoup parlé, une personne, actuellement sur la

liste des criminels les plus recherchés du FBI, aurait recruté des pirates informatiques, pour lancer, au moyen de botnets de 5 000 à 10 000 machines des attaques par déni de service contre les concurrents de sa société.<sup>146</sup> Certaines évaluent à 40 à 80 % le volume total de spam retransmis par des botnets.<sup>147</sup> En 2005, des botnets auraient été utilisés pour détourner la campagne publicitaire des « Adwords » de Google, en gonflant artificiellement le nombre d'affichages d'une publicité.<sup>148</sup>

Un certain nombre de spécialistes de la sécurité cités dans divers articles de presse indiquent que des botnets peuvent être loués sur Internet par l'intermédiaire du courrier électronique, de pages Web et des réseaux IRC (*Internet relay chat*).<sup>149</sup> Une de ces offres proposait la location d'un botnet de 5 000 machines pour USD 300.<sup>150</sup> Un certain nombre de spécialistes de la sécurité cités dans divers articles de presse indiquent que des botnets de 1 000 machines peuvent être loués pour une centaine d'USD de l'heure.<sup>151</sup> Les exigences des racketteurs varient en fonction des pertes que les pirates pensent pouvoir infliger à une entreprise en mettant hors service son site Web. Ainsi, un attaquant aurait déclaré à un agent de la *National Hi-Tech Crime Unit*, se faisant passer pour un autre pirate, qu'il demandait de USD 5 000 à 10 000 pour mettre fin à ses attaques, selon la taille du site.<sup>152</sup> Certaines entreprises font état de demandes d'extorsion de USD 30 000 à 50 000, sous la menace d'attaques par déni de service.<sup>153</sup>

### ***Prise de contrôle du modem***

Il y a « prise de contrôle du modem » quand un internaute télécharge à son insu des programmes qui commandent à son modem de se déconnecter de son FAI pour composer des numéros de téléphone situés dans des pays étrangers, ce qui se traduit par la facturation de frais élevés de téléphone et de services.<sup>154</sup> Ce type d'opération s'effectue à l'insu de l'utilisateur ou sans son consentement, et certains services peuvent facturer jusqu'à USD 500 la minute.<sup>155</sup>

Les programmes exécutables téléchargés en cas de prise de contrôle du modem sont appelés des composeurs Web ou composeurs pirates. Entre août 2003 et août 2004, McAfee a signalé avoir détecté environ 250 000 composeurs Web et 4 millions d'ordinateurs infectés.<sup>156</sup> En 2004, BT a mis en place un nouveau dispositif destiné à lutter contre ce phénomène. Sur les quatre premiers mois de fonctionnement, BT a dû faire face à 45 000 cas de clients dont les factures avaient été gonflées par prise de contrôle de leur modem.<sup>157</sup> Des exemples analogues abondent dans toute la zone de l'OCDE. En 2004, l'Agence finlandaise de protection des consommateurs a traité une affaire dans laquelle des utilisateurs répondant à un test sur Internet étaient déconnectés de leur FAI et reconnectés vers un prestataire danois.<sup>158</sup> En février 2005, l'*Internet Storm Center* a signalé des cas de prise de contrôle de modems en Italie.<sup>159</sup> Dans cet affaire, l'ISC raconte qu'une entité italienne, sous couvert d'un acheteur de domaine aux États-Unis, avait déployé des composeurs qui allaient chercher des éléments supplémentaires de programme sur un site moldave puis essayaient de composer divers numéros de téléphone dans le Pacifique sud.

Bien que l'on dispose de données sur la prise de contrôle de modems auprès d'entreprises comme McAfee et BT en ce qui concerne leurs propres activités, il y a peu de données systématiques disponibles sur ce phénomène. Il existe toutefois un service consacré à l'éducation des utilisateurs au sujet de la fraude par téléphone, en relation avec le programme canadien « Phone Busters ». Phone Busters est une initiative conjointe de la Gendarmerie Royale du Canada, la police provinciale de l'Ontario et le Bureau de la concurrence Canada. Tout un ensemble de statistiques et d'informations sur la fraude téléphonique sont consultables sur le site Web de Phone Busters.<sup>160</sup> La prise de contrôle du modem ne devrait pas constituer un risque pour les internautes disposant d'une connexion à haut débit, à moins qu'il n'ait également une connexion par réseau commuté.

***Fraude par clic et « référencement abusif »***

Avec le développement du World Wide Web, la publicité est devenue l'un des principaux moyens par lequel les entreprises s'efforcent de rentabiliser leurs investissements dans la prestation de services. Les prestataires de services populaires comme le courrier électronique sur le Web, les moteurs de recherche, l'hébergement de blogs, etc. s'appuient de plus en plus sur les recettes procurées par la publicité. L'un des modèles utilisés consiste pour les gestionnaires de sites à faire payer les publicitaires ou les commerçants pour héberger des liens publicitaires vers leurs propres sites Web. Un paiement est perçu chaque fois qu'un internaute clique sur le lien pour accéder au site. Des paiements complémentaires peuvent être ensuite effectués si l'internaute poursuit sa navigation sur le site pour acheter un produit ou un service.

Un autre modèle consiste pour les publicitaires et commerçants à acheter des mots clés auprès des moteurs de recherche, celui qui fait l'offre la plus élevée ayant sa publicité placée au premier rang à côté des résultats du moteur de recherche. Overture, par exemple, fournit un outil avec lequel les publicitaires peuvent voir combien de fois un mot a été recherché au cours du mois précédent.<sup>161</sup> En janvier 2005, le mot clé « refinace » a été recherché 582 803 fois. Le prix le plus élevé qu'un publicitaire était disposé à payer en février 2005 était de USD 12.04, l'offre suivante étant de USD 12.03, etc. Dans l'hypothèse où un publicitaire ne plafonnerait pas sa dépense à un certain montant et bénéficierait d'un taux de clic de 5 %, la somme totale payable à Overture serait de USD 350 847.

Avec l'essor du marché publicitaire sur Internet, de nouvelles incitations financières à cibler différents segments sont apparues pour les fraudeurs et autres personnes mal intentionnées. La fraude au clic consiste généralement pour un individu à cliquer sur un lien sponsorisé de manière à accroître le montant qui lui est dû.<sup>162</sup> Dans le système d'Overture, il peut également arriver qu'une personne, pour telle ou telle raison, cherche à gonfler les coûts pour un publicitaire et à l'évincer du classement fourni par le moteur de recherche une fois que son plafond annuel a été atteint. Cela peut soit se faire manuellement, en s'adressant à des sous-traitants à bas coûts, soit au moyen de logiciels automatiques ou d'un botnet. Ce phénomène attire déjà l'attention des chercheurs universitaires qui souhaitent comprendre l'efficacité du « spam sur les liens ».<sup>163</sup>

La fraude au clic peut varier selon la façon dont le moteur de recherche place les publicités. À la différence d'Overture, par exemple, Google prend semble-t-il en compte les taux de clic (CTR) pour décider du classement des publicités dans son moteur de recherche. Avec ce système, des affichages supplémentaires sans clic peuvent conduire au déclassement d'une publicité, ou même à sa désactivation. La pratique alléguée, à propos des résultats de Google, consiste pour un fraudeur à « ... exploiter le système Google en mettant temporairement en pause ses propres campagnes « adware », en inondant certains mots-clés sur lesquels il est positionné puis en réactivant ses publicités. Cela entraîne une baisse du taux de clic de ses concurrents et lui permet de bénéficier d'un meilleur positionnement à un prix plus faible ».<sup>164</sup> Cette pratique sur le moteur Google est appelée spam par affichage (impression spam).

Un nombre croissant d'articles de presse indiquent que la fraude au clic est une menace sur la confiance des acheteurs d'espaces publicitaires.<sup>165</sup> Fin 2004, le Responsable financier de Google aurait selon certains déclaré à une conférence d'investisseurs qu'il fallait agir rapidement contre la fraude au clic en raison du risque qu'elle présente pour le modèle économique de l'entreprise.<sup>166</sup>

La mesure du spam dans le courrier électronique n'est pas prise en compte dans le présent rapport car des travaux se poursuivent ailleurs. Le référencement abusif ou « spam de contenu » apparaît toutefois de plus en plus comme un problème pour les propriétaires de sites Web, de blogs, de forums et autres médias en ligne qui offrent aux visiteurs la possibilité de poster des commentaires ou d'autres informations. Les objectifs des spammeurs de contenu peuvent être multiples notamment, en sus des motivations traditionnelles, l'amélioration de leur positionnement dans les moteurs de recherche en vue d'obtenir des

recettes plus élevées en améliorant leur taux de clic, ou d'influer sur le marché secondaire des noms de domaine.<sup>167</sup> Une autre motivation peut être la transmission de codes malveillants. Si les spammeurs de contenu peuvent améliorer le classement de leur site Web dans les résultats de recherche, la probabilité augmente que des utilisateurs cliqueront vers ces sites et verront leur système infecté.<sup>168</sup> Des développements tels que celui-ci sont susceptibles d'entamer la confiance qu'ont les utilisateurs dans des outils comme les moteurs de recherche. De nouvelles formes de spam apparaissent également dans des domaines comme la messagerie électronique (à savoir spam sur les messageries instantanées ou « spim »), les blogs (« spam de commentaires ») et le spam sur les téléphones mobiles cellulaires ou la téléphonie par Internet.

### *Mesure de la fraude au clic et du référencement abusif*

L'*Interactive Advertising Bureau*, qui est un groupement professionnel basé aux États-Unis, a défini un ensemble de principes directeurs pour la mesure des campagnes publicitaires en ligne et leur audit.<sup>169</sup> Le groupe d'étude de l'IAB sur les méthodes de mesure travaille sur des normes pour mesurer les taux de clic et éliminer les enregistrements truqués.<sup>170</sup> Une autre source d'information sur le phénomène de la fraude au clic et le spam de contenu est la *Search Engine Marketing Professional Organization* (SEMPO). La publication annuelle de la SEMPO sur l'état du marketing via les moteurs de recherche contient des résultats d'enquête concernant aussi bien la taille du marché de la publicité sur les moteurs de recherche que les opinions des publicitaires et agences de marketing utilisant les moteurs de recherche sur des menaces potentielles comme la fraude au clic et le spam de contenu.<sup>171</sup> Il est intéressant de noter que les personnes interrogées en 2004 ont classé le « spam de contenu » comme une menace plus grande pour la confiance des publicitaires que la fraude au clic.

En février 2005, le *Pew Internet & American Life Project* a publié les résultats d'une enquête sur le phénomène du « spim ».<sup>172</sup> L'étude indiquait que quelque 42 % des 134 millions d'internautes adultes aux États-Unis utilisent la messagerie électronique et près d'un tiers de ces utilisateurs de la messagerie électronique (30 %) ont reçu des « spims ».<sup>173</sup> Le même mois, étaient publiés les premiers résultats d'une enquête auprès des utilisateurs de téléphone mobile concernant leur attitude à l'égard du spam, à l'initiative de l'université de St.Gallen ainsi que de « bmd wireless » et de l'UIT (Union internationale des télécommunications).<sup>174</sup> L'étude indiquait que 83 % des déclarants appartenant à l'industrie des télécommunications considéraient que le spam sur mobile serait un problème critique dans un avenir proche.

## **Sécurité et certification de l'infrastructure de commerce électronique**

### *Secure socket layer (SSL)*

C'est Netscape qui a développé le protocole *Secure Socket Layer* (SSL) pour la transmission de données chiffrées sur les réseaux TCP/IP. L'utilisation la plus courante de SSL consiste à assurer une liaison sécurisée de bout en bout pour les transactions de commerce électronique, les principales applications pour le commerce électronique de ce logiciel de serveur sécurisé étant les transactions chiffrées par cartes de crédit dans les applications de vente de détail et l'accès contrôlé à des informations protégées tant à l'intérieur des organisations qu'entre ces dernières. Le protocole de sécurité SSL assure le chiffrement des données, l'authentification des serveurs, l'intégrité des messages et l'authentification optionnelle des clients dans une connexion TCP/IP.<sup>175</sup> Comme le protocole SSL est intégré dans tous les grands navigateurs et serveurs Web, il suffit d'installer un certificat numérique pour activer leurs fonctions SSL.

L'utilisation de SSL par les sites de commerce électronique est devenue un outil important pour renforcer la confiance entre ces sites et avec leurs clients sur Internet. La FTC, par exemple, recommande

que les consommateurs recherchent les signes (par exemple, l'image d'un cadenas dans la barre d'état du navigateur ou l'URL d'un site Web commençant par https) montrant qu'un site est sécurisé, avant de communiquer des informations personnelles ou financières sur ce site.<sup>176</sup> Des commerçants tels qu'Amazon.com ou des chaînes d'hôtels comme celles appartenant au groupe européen Accor (par exemple, Sofitel, Novotel, Mercure) utilisent de façon systématique des serveurs sécurisés dans le cadre de leurs activités. Les sites de commerce électronique appartenant à ces entreprises affichent couramment des informations semblables à celles reproduites ci-dessous, reprises du site Web de lastminute.com:

« Au moment où vous passez votre commande, vous accédez à des pages entièrement sécurisées... lorsque vous procédez au règlement de vos achats par carte bancaire, les données que vous saisissez sur le formulaire de commande (nom, prénom, adresse, numéro de carte bancaire...) sont cryptées au cours de leur transmission. Ce cryptage permet de garantir une totale sécurité. Pour ce faire, nous utilisons le procédé de cryptage le plus performant du marché, le SSL.

... Par l'usage de techniques cryptographiques, telles que les cryptages et la signature digitale, ces protocoles :

- permettent au browser et au serveur du Web de vous authentifier ;
- autorisent les propriétaires des sites de contrôler l'accès à des serveurs, en particulier, des répertoires, documents en service ;
- permettent à des informations confidentielles d'être échangées entre browser et serveur tout en restant inaccessibles à des tiers ;
- et s'assurer à ce que les échanges de données entre browser et serveur ne puissent pas être corrompus, de manière accidentelle ou intentionnelle sans détection. »<sup>177</sup>

Un élément indispensable dans l'établissement de sessions sécurisées par SSL sur le Web est le certificat à clé public. En signant numériquement les certificats qu'elle délivre, l'autorité de certification lie l'identité du détenteur du certificat à la clé publique contenue dans le certificat et donc garantit l'authenticité du certificat. Des commerçants en ligne comme lastminute.com affichent fréquemment le sceau de l'autorité de certification sur leur site.<sup>178</sup> Il est possible d'utiliser des serveurs sécurisés sans certificat numérique (par exemple pour les transferts d'informations à l'intérieur d'un groupe fermé d'utilisateurs). Toutefois, le fait qu'un site ait pris la peine de mettre en place un processus de certification aurait tendance à indiquer qu'il échange des informations sensibles avec des interlocuteurs extérieurs comme c'est le cas dans le commerce électronique.

Parmi les autorités de certification figurent des sociétés telles que Verisign, GeoTrust, Comodo et Entrust. Verisign est de toutes les autorités de certification celle qui de loin détient la plus forte part du marché. En juillet 2004, avec sa filiale Thawte, Verisign a assuré 39 % de l'ensemble des certifications SSL (annexe 3, tableau 14). La part de marché globale de Verisign est toutefois encore supérieure à cela, car elle signe également certains certificats comme RSA Data Security. A la même date, les principaux concurrents de Verisign, GeoTrust et Comodo, délivraient respectivement 19 % et 11 % de l'ensemble des certificats SSL. La position de Verisign comme premier acteur mondial tient en partie au fait que les premières versions des navigateurs de Netscape et de Microsoft n'acceptaient que des certificats de Verisign. Les versions récentes de ces navigateurs permettent aux utilisateurs d'ajouter ou de retirer des autorités de certification. Cela a suscité une plus grande concurrence sur le marché de la certification, notamment au niveau national où des entreprises détentrices de marques locales de confiance sont entrées sur le marché.

Le coût de la certification a baissé de façon spectaculaire même si la marque Verisign peut se permettre de vendre plus cher ses certificats.<sup>179</sup> En septembre 2004, Verisign demandait USD 349 par an pour le service de chiffrement SSL sur 40 bits d'un site sécurisé, et USD 895 pour un service à 128 bits. Certains concurrents associent la certification SSL à d'autres services et facturent des prix aussi bas que USD 25 pour promouvoir l'utilisation de leurs autres produits (par exemple, des services d'hébergement).<sup>180</sup> En septembre 2004, GoDaddy, qui est un important organisme de gestion de noms de domaine facturait USD 29.95 pour une certification SSL sur 128 bits.<sup>181</sup> EV1Services proposait à la même date une première émission de certificats SSL pour une somme aussi modique que USD 4.95, pour un service à 128 bits.<sup>182</sup> La grande diversité des tarifs constatée sur le marché de la certification SSL tient au fait que des prestataires sont prêts à vendre à perte pour attirer des clients, tandis que certaines marques exploitent leur notoriété sur le marché. Une modulation des tarifs s'est également mise en place, selon que le propriétaire du site Web veut un certificat SSL validé pour son domaine ou validé pour son organisation.

Les certificats validés pour l'organisation impliquent pour l'acquéreur du certificat une procédure de contrôle plus longue et plus exhaustive, ce qui est intéressant pour des opérateurs de sites souhaitant offrir le niveau d'assurance le plus élevé à leurs utilisateurs quant à la sécurité de l'utilisation de leur site.<sup>183</sup> Selon Netcraft, société privée qui réalise la plus importante enquête en ligne sur les serveurs sécurisés, la « ...question clé pour l'avenir sera de savoir si les acquéreurs de certificats SSL continuent d'opter pour des certificats de domaines, moins chers, ou si les inquiétudes suscitées par l'hameçonnage et les autres menaces liées à la sécurité incitent les opérateurs à payer un peu plus pour passer au certificat assurant une certification au niveau de l'organisation. Actuellement, la plupart des acquéreurs de certificats considèrent que leur clientèle ne fait pas de différence entre les deux méthodes de validation ». <sup>184</sup> Cela pourrait toutefois changer dans la mesure où les éditeurs de logiciels de navigation, comme Firefox et Opera, mettent davantage en évidence les fonctions SSL dans leurs fenêtres de navigation comme moyen supplémentaire de renforcement de la sécurité.

Des données sur les parts de marché de la certification SSL et les types de certification peuvent être obtenues auprès de Netcraft. La société rend également disponible pour ses clients des données par pays. Cela permet aux analystes non seulement de voir quels sont les principaux acteurs mondiaux, mais aussi d'avoir une ventilation des données sur les parts de marché par pays. En Allemagne, par exemple, *TC Trust Center for Security in Data Networks GmbH* et *Deutsche Telekom* sont aussi des acteurs majeurs, en plus des grands acteurs mondiaux opérant sur ce marché.

À ce jour, la plupart des utilisations de SSL ont été associées à l'accès à Internet par réseau fixe. Or les réseaux mobiles cellulaires sont de plus en plus à même de proposer des services de commerce électronique. Au Japon, NTT DoCoMo a lancé le service par carte à puce FeliCa, et des combinés compatibles FeliCa peuvent être utilisés pour une diversité d'applications, précédemment réalisables uniquement avec des cartes à puce, notamment achat de billets, transactions de cartes de débit et de crédit, identification personnelle et gestion d'accès à des bâtiments.<sup>185</sup> Des autorités de certification, en vue de faciliter le développement de ce marché, ont commencé à offrir des services SSL ciblés sur les équipements sans fil. En juillet 2004, GeoTrust a commencé à offrir des services de certification SSL destinés à fournir des informations de type Web au marché de la téléphonie mobile (par exemple, pour ordinateurs portables et téléphones intelligents).<sup>186</sup>

L'enquête SSL de Netcraft permet également de connaître sur une base mensuelle le nombre effectif de serveurs sécurisés par pays et, parmi tout un ensemble d'autres indicateurs, le niveau de chiffrement utilisé par chaque serveur sécurisé. En juillet 2004, on dénombrait 305 000 serveurs sécurisés dans la zone de l'OCDE (annexe 3 ; tableau 15). Un peu moins des deux tiers de ces serveurs sécurisés sont implantés aux États-Unis. Ces données peuvent être pondérées en fonction de la population pour faciliter la comparaison du niveau relatif d'adoption de SSL dans l'ensemble des pays membres. En juillet 2004, c'est en Islande, aux États-Unis et au Canada que les taux de déploiement de SSL pour 100 000 habitants étaient

les plus élevés. Un facteur à garder en mémoire lors de l'interprétation du taux d'adoption des serveurs sécurisés est que dans certains pays l'utilisation centralisée de serveurs sécurisés est plus développée que dans d'autres. Dans les pays nordiques, par exemple, les commerçants peuvent ne pas disposer de leur propre serveur sécurisé, les paiements s'effectuant par l'intermédiaire du serveur sécurisé de la banque du consommateur.<sup>187</sup> Aux États-Unis, et dans de nombreux autres pays, les commerçants utilisent PayPal pour le commerce électronique. Avec PayPal, les commerçants n'ont pas besoin d'installer leur propre serveur sécurisé. Paypal se charge de chiffrer automatiquement la communication entre les commerçants et les utilisateurs, via ses propres serveurs sécurisés.

L'enquête sur les serveurs sécurisés de Netcraft repose sur la méthodologie suivante. Chacun des sites dont Netcraft reçoit une réponse positive pour son enquête sur les serveurs Web, ainsi qu'un certain nombre de sites que Netcraft pense susceptibles d'offrir des services exclusivement chiffrés SSL sont interrogés au moyen d'une requête SSL pour récupérer le certificat du site et la signature du serveur au moyen d'un client SSL offrant toute la gamme des chiffrements. Cette information est ensuite automatiquement exploitée pour obtenir des informations telles que l'implantation géographique, le système d'exploitation, l'autorité de certification, le niveau des chiffrements, etc. Il faut noter qu'un changement de méthodologie, en octobre 2001, a introduit une définition plus stricte des sites authentifiés. Les données des enquêtes précédentes n'ont pas été ajustées, de sorte que la comparaison des données d'enquête sur la période 1998 à 2004 est susceptible de légèrement sous-évaluer la progression.

## ANNEXE 1 : QUELQUES STATISTIQUES OFFICIELLES SUR LA CONFIANCE (VIS-À-VIS DE L'ENVIRONNEMENT CONNECTÉ)

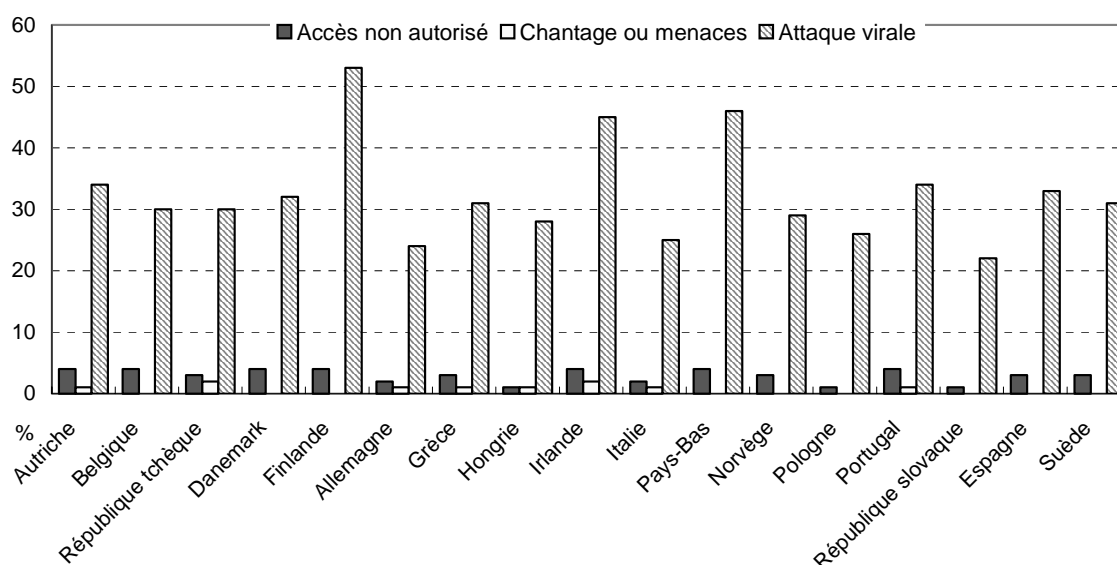
### Eurostat

Nous fournissons ci-après quelques exemples des données Eurostat (figures 1, 2, 3 et 4). Eurostat possède d'autres informations sur ce thème qui sont disponibles sur son site Internet New Cronos.<sup>188</sup>

### Données des entreprises sur la sécurité informatique

Figure 1. **Pourcentage d'entreprises disposant d'un accès à Internet ayant rencontré des problèmes de sécurité en 2004**

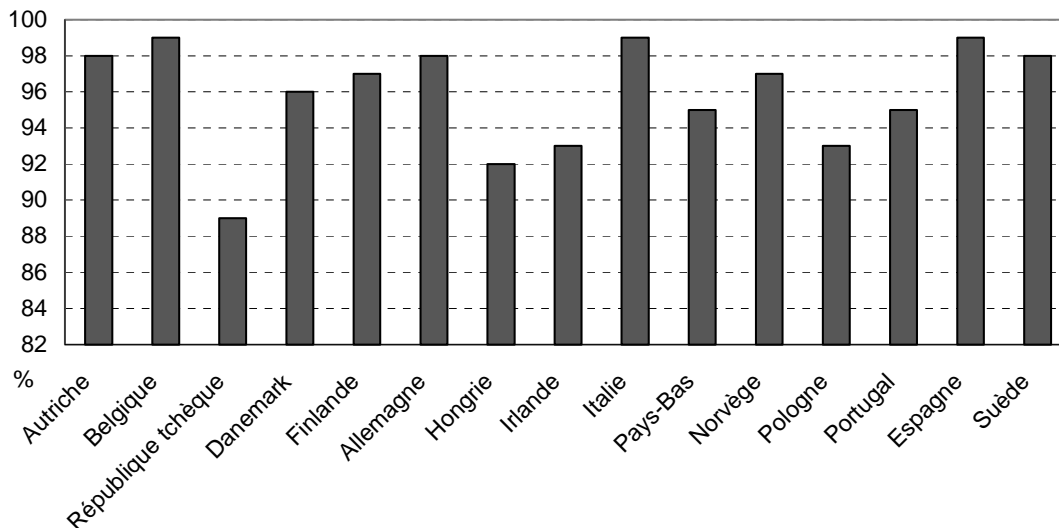
Pourcentage d'entreprises comptant au moins 10 salariés et ayant accès à Internet



Source : Eurostat, Enquête communautaire sur l'usage des TIC dans les entreprises, 2003, février 2005.

Figure 2. **Pourcentage d'entreprises disposant d'un accès à Internet et ayant pris des mesures de sécurité en 2004**

Pourcentage d'entreprises comptant au moins 10 salariés et ayant accès à Internet

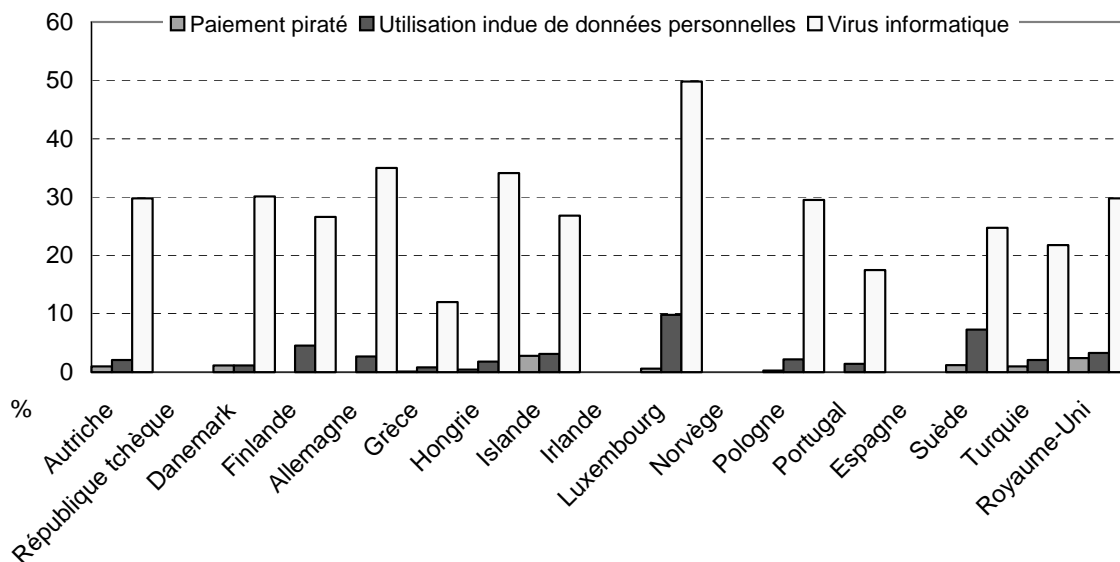


Source : Eurostat, Enquête communautaire sur l'usage des TIC dans les entreprises, 2004, février 2005.

*Données des ménages sur la sécurité informatique*

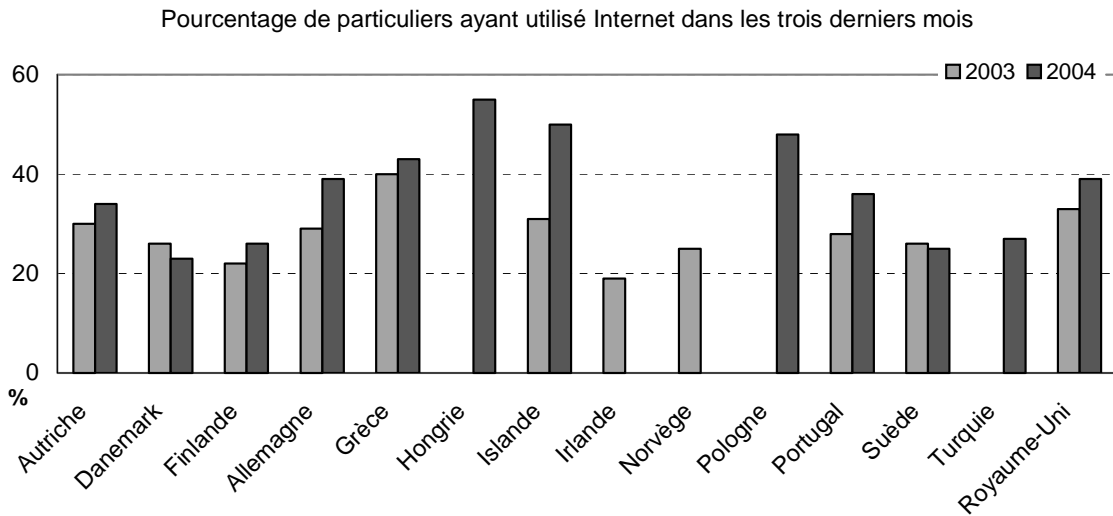
Figure 3. **Pourcentage de particuliers internautes ayant rencontré des problèmes de sécurité en 2004**

Pourcentage de particuliers ayant utilisé Internet au cours de l'année écoulée



Source : Eurostat, Enquête communautaire sur l'usage des TIC par les ménages et les particuliers, 2004, février 2005.

Figure 4. **Pourcentage de particuliers ayant, dans les trois derniers mois, installé un programme de détection virale**

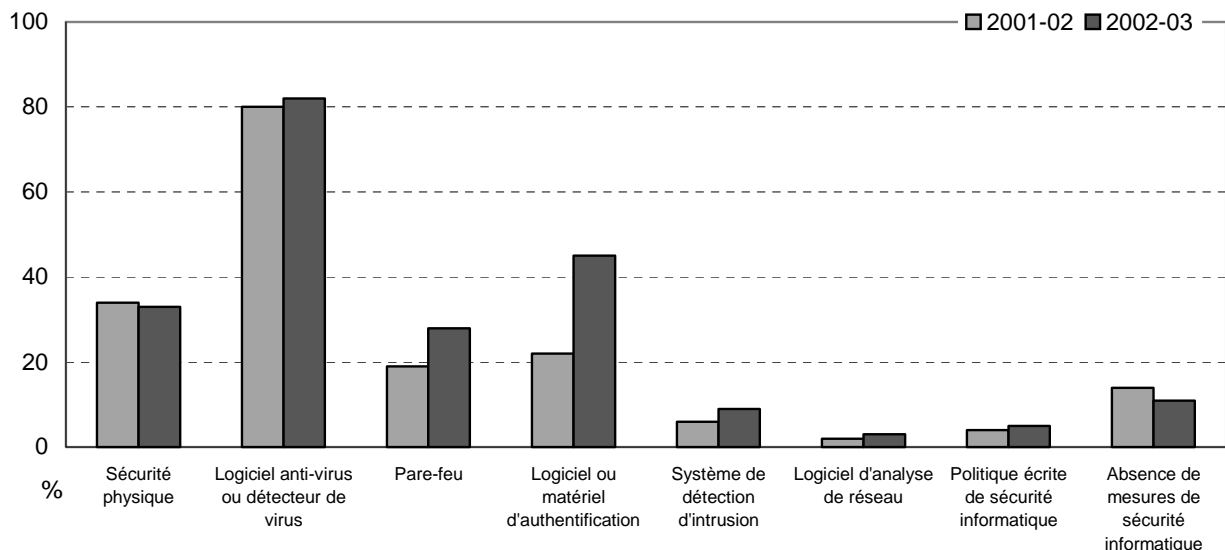


Source : Eurostat, Enquête communautaire sur l'usage des TIC par les ménages et les particuliers, 2003 et 2004, février 2005.

## Australie

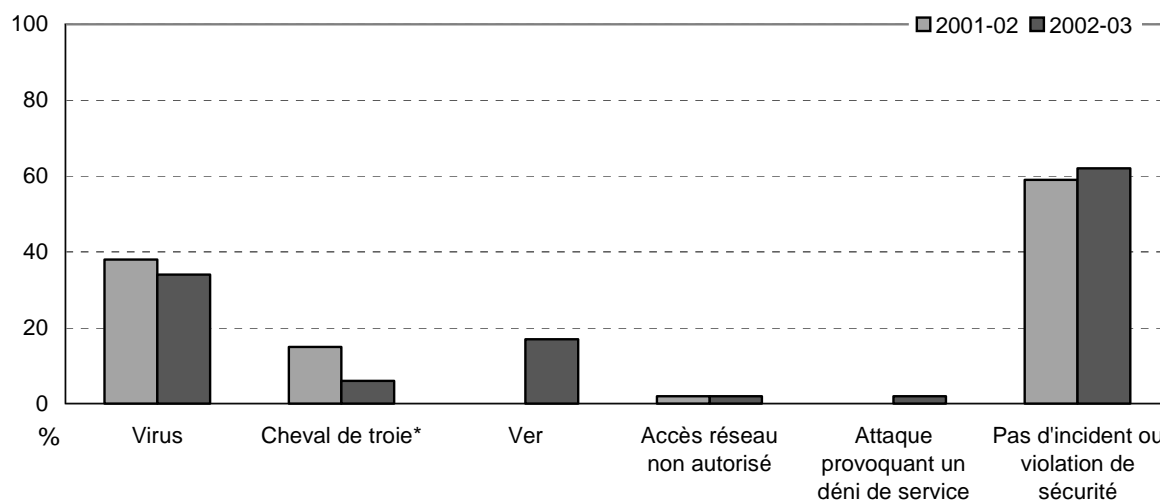
Dans son *Business Use of Information Technology Survey* (enquête sur l'utilisation de l'informatique par les entreprises) annuelle, l'*Australian Bureau of Statistics* (ABS) a recueilli auprès des entreprises des données sur la sécurité informatique pour les périodes 2001-02 et 2002-03. Nous présentons ci-après quelques-uns des résultats obtenus (figures 5 et 6). Les publications complètes sont disponibles sur le site Internet de l'ABS.<sup>189</sup>

Figure 5. **Mesures de sécurité appliquées par les entreprises en 2001-02 et 2002-03**  
Pourcentage d'entreprises informatisées déclarant appliquer des mesures de sécurité



Source : Australian Bureau of Statistics, *Business Use of Information Technology*, 2000-01 et 2002-03, cat. n° 8129.0.

Figure 6. **Entreprises ayant rapporté des incidents ou violations de sécurité informatique en 2001-02 et 2002-03**  
 Pourcentage d'entreprises informatisées ayant rapporté des incidents ou des violations de sécurité



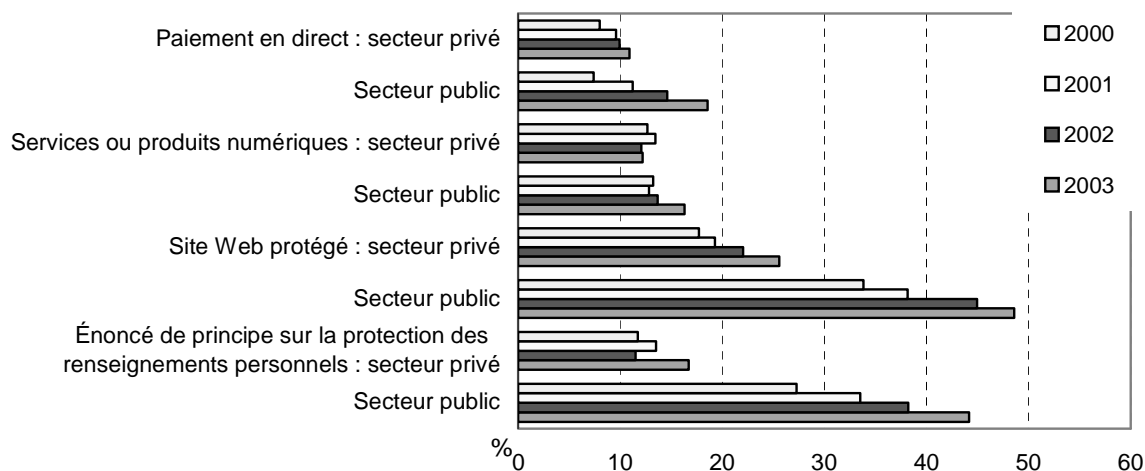
\*Pour 2001-02, la catégorie Cheval de Troie inclut les vers.

Source : Australian Bureau of Statistics, *Business Use of Information Technology*, 2000-01 et 2002-03, cat. n° 8129.0.

### Canada

Statistique Canada mène chaque année une *Enquête sur le commerce électronique et la technologie* qui lui permet de recueillir des données sur l'utilisation des TIC dans les entités des secteurs tant privé que public (hors collectivités locales). Cette enquête comporte entre autres des questions portant sur l'existence, sur le site Internet de l'entité, d'une déclaration concernant la politique appliquée en matière de respect de la confidentialité des données personnelles, ainsi que sur la sécurité du site, c'est-à-dire sur l'existence de politiques et de technologies (par exemple SSL et PKI [infrastructure à clé publique]) destinées à sécuriser les transactions ou les informations. Nous en présentons quelques résultats ci-après (figure 7).

Figure 7. **Caractéristiques des sites Internet dans les secteurs public et privé, 2000 à 2003**  
 Pourcentage d'entreprises dont le site présente ces caractéristiques



Source : Statistique Canada, *Enquête sur le commerce électronique et la technologie*, 2000 à 2003.

## Japon

L'enquête sur les tendances de l'utilisation des communications qu'a menée le Japon en 2003 auprès des ménages et des entreprises comporte un certain nombre de questions sur la confiance. Les données 2003 sont publiques ;<sup>190</sup> consultez les figures 6-11 (qui concernent tant les ménages que les entreprises). Les questionnaires utilisés pour cette enquête sont également disponibles.<sup>191</sup>

## États-Unis

Dans son supplément sur l'informatique et Internet, l'enquête américaine du Bureau du recensement sur la population d'octobre 2003 a adopté une démarche différente de celle d'autres enquêtes en posant des questions sur l'inquiétude qu'éprouvent les interviewés lorsqu'ils fournissent des renseignements personnels sur Internet (par rapport au téléphone) et vis-à-vis du contenu auquel sont exposés les enfants sur Internet (par rapport à la télévision). Nous présentons ces résultats ci-après (tableaux 1 et 2). D'autres résultats de cette enquête sont disponibles dans le rapport 2004 intitulé *A Nation On-line: Entering the Broadband Age*.<sup>192</sup>

Tableau 1. Inquiétude concernant la fourniture de renseignements personnels par téléphone et sur Internet, octobre 2003, États-Unis

Par rapport au téléphone, à quel point redoutez-vous de fournir des renseignements personnels sur Internet ?							Total	
	16-24 ans	25-44 ans	45-64 ans	65-74 ans	Hommes*	Femmes*	Ensemble*	Internautes*
Davantage	46.1	45.8	52.3	57.2	48.1	49.8	49.0	47.4
Moins	8.2	8.7	7.7	6.5	8.5	7.8	8.1	7.7
À peu près autant	45.7	45.5	40.0	36.3	43.4	42.4	42.9	44.8

\*Âgés de 16 à 74 ans.

Source : US Department of Commerce, Economic and Statistics Administration, Computer and Internet Supplement to the Current Population Survey, octobre 2003, information non publiée.

Tableau 2. Inquiétude concernant l'exposition des enfants au contenu de la télévision et d'Internet, octobre 2003, États-Unis

Par rapport à la télévision, à quel point redoutez-vous les contenus auxquels les enfants peuvent être exposés sur Internet ? (question posée aux seuls interviewés dont le foyer compte des enfants de moins de 18 ans)							Total	
	16-24 ans	25-44 ans	45-64 ans	65-74 ans	Hommes*	Femmes*	Ensemble*	Internautes*
Davantage	68.8	69.1	73.4	75.0	69.5	70.5	70.0	72.3
Moins	6.1	5.8	4.5	1.0	5.5	5.6	5.5	5.3
À peu près autant	25.1	25.1	22.1	24.0	25.0	24.0	24.5	22.4

\*Âgés de 16 à 74 ans.

Source : US Department of Commerce, Economic and Statistics Administration, Computer and Internet Supplement to the Current Population Survey, octobre 2003, information non publiée.

## ANNEXE 2 : PROJET DE QUESTIONS OCDE TYPES SUR LA CONFIANCE

Les enquêtes types de l'OCDE sur l'utilisation des TIC par les entreprises et les ménages/particuliers sont en cours de révision. Au moment où nous rédigeons ces lignes, les projets comportent un certain nombre de questions relatives à la confiance dans l'environnement en ligne. Les propositions contiennent par ailleurs, sur la mesure d'autres thèmes concernant la confiance, des points de discussion dont nous fournissons les détails ci-après.

### Projet de questionnaire OCDE type concernant l'utilisation des TIC par les entreprises (arrêté à avril 2005)

Un questionnaire type révisé sur l'usage des TIC par les entreprises a été présenté lors de la réunion d'avril 2005 du Groupe de travail sur les indicateurs de la société de l'information (GTISI) [DSTI/ICCP/IIS(2005)2, document de travail interne]. Ce questionnaire donnera lieu à d'autres modifications résultant des débats de cette réunion et des commentaires écrits qui l'auront suivie.

Nous reproduisons ci-après les questions concernées par le projet d'avril. Un bref rapport reprenant les réactions des délégués, et notamment les conséquences probables sur les questions proposées, est présenté ensuite.

#### *Section A : informations générales sur l'utilisation des TIC par votre entreprise*

La question 8 de la section A est posée aux entreprises présentes sur Internet (ce qui suppose la détention d'un site ou d'une page d'accueil sur Internet, ou une présence sur un site tiers (y compris d'une entité affiliée) dont le contenu (qu'il s'agisse de tout le site ou d'une page) est contrôlé de manière substantielle par l'entreprise).

#### À <date de référence>, la présence de votre entreprise sur Internet s'accompagnait-elle ?

Cochez toutes les réponses utiles

- |   |                          |   |
|---|--------------------------|---|
| D'une déclaration de politique en matière de sécurité | <input type="checkbox"/> | Une déclaration de politique en matière de sécurité explique les mesures de sécurité qui ont été prises et peut faire référence à la sécurité des renseignements détenus sur le client (durant leur transmission ou leur stockage) ou des transactions financières. |
| D'un sceau ou d'une certification de sécurité         | <input type="checkbox"/> | Fait référence à la certification du niveau de sécurité par une tierce partie. Peut aussi être appelé label de confiance.   |
| D'une déclaration de politique de confidentialité     | <input type="checkbox"/> | Peut être appelée programme, notice ou garantie de confidentialité. Explique les pratiques de l'entreprise en matière de manipulation et d'utilisation des renseignements personnels.   |
| D'un sceau ou d'une certification de confidentialité  | <input type="checkbox"/> | Fait référence à la certification du respect des données personnelles attribuée par une tierce partie. Peut aussi être appelé label de confiance.   |

**Section B : sécurité informatique**

Les questions 9 et 10 concernent la sécurité informatique. Voici leur rédaction projetée :

**À <date de référence>, votre entreprise avait-elle mis en œuvre les mesures de sécurité informatique suivantes ?**

Cochez toutes les réponses utiles

- |   |                          |  |
|---|--------------------------|--|
| Logiciel de détection ou de protection virale régulièrement mis à jour                      | <input type="checkbox"/> | Logiciel détectant et prenant en charge les programmes malveillants tels que les virus, chevaux de Troie et vers. La mise à jour régulière désigne le téléchargement automatique ou manuel de définitions de virus.                            |
| Logiciel anti-espionnage  | <input type="checkbox"/> | Logiciel détectant et supprimant les logiciels espions présents sur un ordinateur (les logiciels espions recueillent des données sur l'utilisateur, à son insu, au travers de sa connexion Internet).  |
| Pare-feu  | <input type="checkbox"/> | Logiciel ou matériel contrôlant les entrées et les sorties d'un réseau ou d'un ordinateur.   |
| Communication client-serveur sécurisée (via par exemple SSL ou SHTTP)                       | <input type="checkbox"/> | SSL est un protocole de chiffrement qui crée une connexion sécurisée entre un client et un serveur. SHTTP prend en charge la transmission sécurisée de messages sur Internet.  |
| Logiciel ou matériel d'authentification pour les usagers internes                           | <input type="checkbox"/> | Les logiciels ou matériels d'authentification vérifient l'identité d'un usager interne ou externe, le périphérique d'un usager ou d'autres éléments. L'authentifiant peut être notamment un mot de passe, un jeton ou une signature numérique. |
| Logiciel ou matériel d'authentification pour les usagers externes (par exemple les clients) | <input type="checkbox"/> |  |
| Système de détection d'intrusion  | <input type="checkbox"/> | Tout système tentant de détecter une intrusion dans un ordinateur ou un réseau par l'observation d'actions, de journaux de sécurité ou de données d'audit.   |
| Sauvegarde régulière des données essentielles au fonctionnement de l'entreprise             | <input type="checkbox"/> |  |
| Sauvegarde des données à l'extérieur de l'entreprise  | <input type="checkbox"/> | Copies de sauvegarde des fichiers informatiques stockées sur un site différent de votre principal lieu de stockage de données.   |
| Programmes de formation des salariés à la sécurité informatique                             | <input type="checkbox"/> |  |
| Autre (veuillez préciser).....  | <input type="checkbox"/> |  |
| Pas de mesures de sécurité en vigueur   | <input type="checkbox"/> |  |

**Votre entreprise a-t-elle connu l'un des problèmes de sécurité informatique suivants durant <période> ?**

**Cette question ne porte pas sur les attaques auxquelles les mesures de sécurité en place ont réussi à parer.**

Cochez toutes les réponses utiles

- |   |                          |  |
|---|--------------------------|--|
| Une attaque par un virus, un cheval de Troie ou un ver                | <input type="checkbox"/> | Se traduisant par une perte de données ou de temps, ou par des dégâts logiciels ou matériels.  |
| Un accès externe non autorisé à vos données ou systèmes informatiques | <input type="checkbox"/> | Pouvant occasionner un usage frauduleux, une extorsion ou un vol d'informations.   |
| Une attaque se traduisant par un déni de service                      | <input type="checkbox"/> | Une attaque par déni de service restreint volontairement l'accès à un système informatique, par exemple en le noyant sous un trafic très important, de sorte qu'il devienne inutilisable de façon normale. |
| Autre (veuillez préciser).....  | <input type="checkbox"/> |  |
| Pas de problème de sécurité informatique                              | <input type="checkbox"/> |  |

**Section C : comment votre entreprise utilise-t-elle les TIC dans son fonctionnement ?**

La question 29 de la section C est une question filtre concernant tous les interviewés qui utilisent des réseaux informatiques. Les catégories de réponses pertinentes sont : *Préoccupations relatives à la sécurité*, *Préoccupations relatives à la confidentialité* et *Incertitudes concernant le cadre juridico-réglementaire du commerce via des réseaux informatiques*.

**Parmi les facteurs suivants, lequel ou lesquels ont, le cas échéant, limité ou empêché des ventes de votre entreprise via Internet ou d'autres réseaux informatiques durant <période> ?**

Cochez toutes les réponses utiles

Les produits de votre entreprise sont mal adaptés au commerce via des réseaux informatiques	<input type="checkbox"/>	
Préoccupations relatives à la sécurité	<input type="checkbox"/>	Comprend les inquiétudes qu'a votre entreprise et les inquiétudes qu'elle perçoit chez ses clients (par exemple à propos de la divulgation de coordonnées de carte de crédit sur Internet).
Préoccupations relatives à la confidentialité	<input type="checkbox"/>	Comprend les inquiétudes qu'a votre entreprise et les inquiétudes qu'elle perçoit chez ses clients (par exemple à propos de la divulgation de renseignements personnels sur Internet).
Préférence pour le maintien du modèle d'activité en vigueur, comme par exemple les contacts en personne	<input type="checkbox"/>	
Incompatibilité des systèmes des clients avec vos propres systèmes	<input type="checkbox"/>	Fait référence aux problèmes d'interopérabilité, qui peuvent aussi être décrits comme des difficultés techniques d'interaction entre les systèmes internes et les systèmes externes.
Demande insuffisante de la clientèle en termes d'achat en ligne sur des réseaux informatiques	<input type="checkbox"/>	
Incertitudes concernant le cadre juridico-réglementaire du commerce via des réseaux informatiques	<input type="checkbox"/>	
Coût du développement ou de la maintenance trop élevé	<input type="checkbox"/>	
Compétences ou formation adaptée insuffisantes	<input type="checkbox"/>	
Le commerce via des réseaux informatiques n'a pas été limité ou empêché.	<input type="checkbox"/>	
Sans objet : la vente via des réseaux informatiques est en cours de développement ou prévue à brève échéance	<input type="checkbox"/>	
Autre (veuillez préciser).....	<input type="checkbox"/>	

*Faisabilité des questions sur la sécurité informatique du questionnaire type*

Les délégués à la réunion 2005 du GTISI ont été invités à s'exprimer sur la faisabilité statistique des projets de questions susmentionnés et sur l'opportunité des thèmes suivants :

- L'entreprise a-t-elle procédé à une évaluation des risques que présente son système informatique du point de vue de la sécurité et, dans l'affirmative, de quel type d'évaluation s'est-il agi (par exemple : interne, par un tiers, par un organisme officiel de certification, etc.) ?
- Les entreprises qui utilisent un logiciel antivirus téléchargent-elles des définitions de virus et, dans l'affirmative, le font-elle automatiquement, chaque jour, chaque semaine, etc. ?

- L'entreprise applique-t-elle les correctifs et mises à jour logiciels qui sont essentiels pour la sécurité de ses systèmes informatiques et, dans l'affirmative, le fait-elle automatiquement, chaque jour, chaque semaine, etc. ?

### *Réactions du Groupe de travail*

Les réactions ont principalement porté sur la faisabilité de la question 10 susmentionnée. Plusieurs pays, ainsi qu'Eurostat, ont indiqué que les entreprises avaient tendance à minimiser, dans leurs réponses, les incidents de sécurité qu'elles avaient connus. C'est pourquoi cette question sera incorporée à la prochaine version du questionnaire, mais en tant que question **secondaire**. Peu de commentaires particuliers ont été faits sur les questions 8, 9 et 29, qui seront donc probablement reprises sous une forme peu différente. Les réactions aux nouveaux thèmes soumis à débat ont été très peu nombreuses, mais les questions sur l'évaluation des risques et la mise à jour des logiciels antivirus font actuellement partie d'un exercice limité de test de questionnaire entrepris par Statistique Canada, dont les résultats sont attendus d'ici la fin du mois d'août.

### **Questionnaire OCDE type révisé concernant l'utilisation des TIC par les ménages et les particuliers (arrêté à août 2005)**

Un questionnaire type révisé sur l'utilisation des TIC par les ménages et les particuliers a été présenté à la réunion du GTISI d'avril 2005 [DSTI/ICCP/IIS(2005)3]. Ce questionnaire a été ensuite révisé en fonction des débats de cette réunion et des commentaires écrits qui l'ont suivie. Les délégués étaient tout particulièrement invités à commenter les projets de questions sur la sécurité informatique et la faisabilité de l'incorporation de nouveaux thèmes. Un bref rapport sur ce dernier point est présenté plus loin.

Nous reproduisons ci-après les questions du projet intégrant les avis des délégués.

### ***Section A : accès des ménages aux technologies de l'information et des communications***

La question 5 de la section A est une question filtre posée aux ménages qui n'ont pas accès (à domicile) à Internet. Les catégories de réponses pertinentes sont : *Préoccupations relatives à la vie privée*, *Préoccupations relatives à la sécurité* et *Préoccupations relatives aux contenus préjudiciables*. Voici la question :

#### **Quelles sont TOUTES les raisons pour lesquelles les membres du ménage n'ont pas accès à l'Internet à domicile ?<sup>10</sup>**

*Population : les ménages entrant dans le champ de l'enquête qui n'ont pas accès à l'Internet à domicile (qu'ils disposent ou non d'un ordinateur)*

Plusieurs réponses sont autorisées

Manque d'intérêt	<input type="checkbox"/>	
Coût trop élevé	<input type="checkbox"/>	De l'équipement comme de l'accès.
Manque de confiance, de connaissances ou de capacités	<input type="checkbox"/>	
Préoccupations relatives aux contenus préjudiciables	<input type="checkbox"/>	Par exemple, crainte que les enfants n'accèdent à des sites qui ne leur conviennent pas.
Accès à l'Internet à partir d'un autre endroit	<input type="checkbox"/>	Par exemple, les membres du ménage sont en mesure d'utiliser l'Internet au travail.

Note : le fait de ne pas disposer d'un ordinateur ne constitue pas une réponse valable.

Préoccupations relatives à la sécurité, par exemple en ce qui concerne les virus

Préoccupations relatives à la vie privée, concernant par exemple l'usage abusif d'informations à caractère personnel

Autres (préciser).....

**Section B : Utilisation des technologies de l'information et des communications par les individus (adultes)**

Les questions 8, 15 et 16 de la section B sont des questions sur la sécurité informatique posées à un individu. La question 8 concerne la sauvegarde des fichiers des ordinateurs utilisés à domicile, et les questions 15 et 16 traitent de la sécurité de l'Internet à domicile. Voici les questions :

**Question 8**

**Si vous avez utilisé un ordinateur à la maison au cours des 12 derniers mois, à quelle fréquence avez-vous sauvegardé les fichiers (documents, feuilles de calcul ou photographies numérisées) que vous avez créés et conservés dans votre ordinateur ?<sup>15</sup>**

*Population : les ménages entrant dans le champ de l'enquête qui ont utilisé un ordinateur à la maison au cours des 12 derniers mois*

Toujours ou presque toujours

Parfois

Jamais ou presque jamais

Sans objet – je n'ai pas créé de fichier que j'ai conservé dans l'ordinateur utilisé à la maison

Par exemple, sur un CD, un « *memory stick* », un lecteur de disque dur externe ou sur des sites Web (par exemple, ceux qui offrent du stockage en ligne pour les photographies et d'autres fichiers). Y compris les fichiers créés ailleurs (par exemple, sur un ordinateur de poche ou un appareil photo numérique) et transférés sur un ordinateur utilisé à la maison.

Autrement dit, tous les fichiers, ou la plupart, qui sont créés par l'individu sont sauvegardés soit ponctuellement, soit dans le cadre d'une opération périodique portant sur les nouveaux fichiers (ou tous les fichiers).

**Question 15**

**Lorsque vous avez utilisé un ordinateur pour accéder à l'Internet à partir de chez vous au cours des 12 derniers mois, avez-vous été victime d'une attaque de virus ou de logiciel malveillant similaire (par exemple, un cheval de Troie ou un ver) qui a entraîné la perte de données ou de temps ?<sup>19</sup>**

*Population : les ménages entrant dans le champ de l'enquête qui ont utilisé un ordinateur pour accéder à l'Internet à partir de leur domicile au cours des 12 derniers mois*

Non    Oui    Je ne sais pas

À l'exclusion des attaques auxquelles les mesures de sécurité mises en place ont paré avec succès.

## Question 16

**Est-ce que l'ordinateur que vous avez utilisé (principalement) pour accéder à l'Internet à partir de chez vous bénéficiait des dispositifs de protection suivants :**

*Population : les ménages entrant dans le champ de l'enquête qui ont utilisé un ordinateur pour accéder à l'Internet à partir de leur domicile au cours des 12 derniers mois*

	Non	Oui	Je ne sais pas	
Logiciel de vérification ou de neutralisation de virus ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Logiciel qui détecte les programmes malveillants tels que les virus, chevaux de Troie et vers, et y riposte.
Pare-feu ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Logiciel ou matériel qui contrôle l'accès à un réseau ou un ordinateur, ou la sortie de ce réseau ou de cet ordinateur.
Système anti-logiciel espion ?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Logiciel qui détecte et neutralise les logiciels espions d'un système informatique (un logiciel espion est un logiciel de traçage qui recueille de l'information à l'insu de l'internaute).

La question 23 de la section B est une question sur les obstacles à l'achat sur Internet visant les particuliers qui sont internautes mais n'ont rien acheté sur Internet (au cours des 12 derniers mois). Les catégories de réponses pertinentes sont les suivantes :

- J'ai des doutes en ce qui concerne la sécurité (par exemple, j'hésite à fournir sur l'Internet des renseignements sur ma carte de débit ou de crédit).
- J'attache de l'importance à la protection de ma vie privée (j'hésite à fournir des renseignements personnels sur l'Internet).
- Je n'ai pas vraiment confiance (je suis préoccupé par les garanties, la réception et le retour des biens ou des services).

**Quelles ont été TOUTES les raisons qui vous ont dissuadé d'acheter ou de commander sur l'Internet au cours des 12 derniers mois des biens ou des services destinés à votre utilisation personnelle ?**

*Population : tous les individus entrant dans le champ de l'enquête qui ont utilisé l'Internet au cours des 12 derniers mois mais qui n'ont ni acheté ni commandé sur l'Internet au cours de cette période des biens ou des services destinés à leur utilisation personnelle.*

Plusieurs réponses sont autorisées

Cela ne m'intéresse pas	<input type="checkbox"/>
Je préfère faire mes achats en personne ou avoir un contact personnel avec le prestataire de services	<input type="checkbox"/>
J'ai des doutes en ce qui concerne la sécurité (par exemple, j'hésite à fournir sur l'Internet des renseignements sur ma carte de débit ou de crédit)	<input type="checkbox"/>
J'attache de l'importance à la protection de ma vie privée (j'hésite à fournir des renseignements personnels sur l'Internet)	<input type="checkbox"/>
Je n'ai pas vraiment confiance (je suis préoccupé par les garanties, la réception et le retour des biens ou des services)	<input type="checkbox"/>
Je manque de confiance, de connaissances ou de capacités	<input type="checkbox"/>
La vitesse de connexion est trop basse	<input type="checkbox"/>
Autres (préciser).....	<input type="checkbox"/>

*Faisabilité de l'incorporation au questionnaire type d'autres éléments concernant la confiance*

Les délégués à la réunion 2005 du GTISI étaient invités à s'exprimer sur la faisabilité technique des types suivants de questions et à relater toute expérience ayant permis de tester ou de poser de telles questions :

- Les ménages qui utilisent un logiciel antivirus téléchargent-ils des définitions de virus et, dans l'affirmative, le font-ils automatiquement, chaque jour, chaque semaine, etc. ? (Une telle question peut être posée au niveau du foyer ou de l'individu.)
- Les ménages appliquent-ils les mises à jour et correctifs logiciels qui sont essentiels pour la sécurité de leur ordinateur et, dans l'affirmative, le font-ils automatiquement, chaque jour, chaque semaine, etc. ? (Une telle question peut être posée au niveau du foyer ou de l'individu.)
- Les particuliers sauvegardent-ils régulièrement leurs fichiers importants (documents, feuilles de calcul, courriels, photos numériques, etc.) ?
- Quelles sources les particuliers utilisent-ils pour trouver des renseignements sur les questions de sécurité informatique (presse écrite, télévision, sites Internet des fournisseurs, sites Internet des pouvoirs publics, etc.) ?

*Réactions du Groupe de travail*

La réaction générale d'Eurostat et d'autres intervenants est qu'il est problématique d'interroger des particuliers sur la sécurité informatique sur les points suivants : incidents rencontrés, action menée pour se protéger, réalité de la protection de l'ordinateur domestique. Les réactions concernant l'incorporation des nouveaux thèmes susmentionnés sont du même ordre : les interviewés seront probablement incapables de répondre à des questions si techniques. La seule exception semble concerner la question de la sauvegarde régulière des fichiers importants : il s'agit d'une question que la Finlande a posée avec succès, et une nouvelle question accessoire (Q8) portant sur ce thème a été rajoutée au questionnaire type. Si les réactions générales aux questions sur la sécurité informatique sont de l'ordre du scepticisme, leur importance pour l'action publique est telle que ces questions ont été conservées, à titre de questions **accessoires**, dans le questionnaire type révisé. Les réactions ont tout de même incité à restreindre les questions 8 (sur la sauvegarde des données) et 15 (sur les incidents rencontrés) à l'**utilisation domestique**, puisqu'il s'agit de l'environnement probablement le mieux connu des usagers et le plus contrôlé par eux (par exemple, ils peuvent n'avoir aucun rôle dans les sauvegardes effectuées sur le lieu de travail, ou aucune connaissance des attaques subies par l'ordinateur utilisé dans l'établissement scolaire).

### ANNEXE 3 : QUELQUES STATISTIQUES SUR LA CONFIANCE ISSUES DE SOURCES PRIVÉES ET SEMI-OFFICIELLES

Tableau 1. Raisons de ne pas acheter sur Internet dans les pays de l'UE, 2003 (%)

	Vous n'avez pas accès à Internet	<b>Vous ne faites pas confiance à Internet</b>	L'utilisation d'Internet est trop chère	Vous ne voyez pas l'intérêt de faire des achats sur Internet	Acheter sur Internet est trop compliqué	Internet est trop compliqué	Vous n'avez pas de carte de crédit	Vous ne comprenez pas suffisamment bien la langue	Autres raisons	NSP
Autriche	58	<b>20</b>	7	34	8	7	10	4	9	0
Belgique	55	<b>31</b>	4	35	5	6	8	2	7	1
Danemark	46	<b>31</b>	4	34	9	8	9	3	7	1
Finlande	46	<b>22</b>	3	41	10	6	12	7	8	3
France	66	<b>31</b>	8	22	8	7	5	2	5	2
Allemagne	64	<b>20</b>	9	36	10	9	7	3	3	2
Grèce	56	<b>27</b>	3	29	4	4	5	5	6	3
Irlande	50	<b>16</b>	4	24	6	5	14	2	5	8
Italie	47	<b>26</b>	3	23	3	4	8	1	5	1
Luxembourg	42	<b>34</b>	3	28	5	7	7	1	8	2
Pays-Bas	36	<b>32</b>	7	33	7	6	16	4	11	1
Portugal	57	<b>20</b>	7	29	6	9	3	3	11	2
Espagne	56	<b>24</b>	3	21	5	5	3	3	4	1
Suède	33	<b>37</b>	4	45	13	6	6	5	7	4
Royaume-Uni	58	<b>22</b>	2	25	5	7	8	2	9	2
<b>UE15</b>	<b>57</b>	<b>25</b>	<b>5</b>	<b>28</b>	<b>7</b>	<b>7</b>	<b>7</b>	<b>2</b>	<b>6</b>	<b>2</b>

Note : cette question a été posée aux 83 % d'interviewés citoyens de l'UE qui n'avaient pas utilisé Internet pour faire des achats.

Source : Commission européenne, sondage Eurobaromètre spécial intitulé *European Union public opinion on issues relating to business to consumer e-commerce* (réf. : 201 EB60.0), mars 2004.

Tableau 2. Inquiétudes relatives aux achats sur Internet dans les pays de l'UE, 2003 (%)

	Sécurité des paiements	Crédibilité des informations sur Internet	Livraison (marchandises endommagées, retard, non-livraison, etc.)	Respects de vos droits en tant que consommateur	Possibilité d'obtenir un remboursement	Anonymat des vendeurs	Je ne suis pas inquiet(ète)	Autres	NSP
Autriche	35	22	26	13	25	19	34	2	0
Belgique	53	20	35	14	32	8	25	1	2
Danemark	41	19	33	18	33	8	31	0	0
Finlande	36	24	34	18	38	28	25	0	2
France	51	20	44	25	36	16	21	0	0
Allemagne	38	32	40	21	42	20	23	0	1
Grèce	50	23	36	8	27	10	25	3	0
Irlande	45	24	21	18	21	8	31	1	2
Italie	61	26	32	19	43	11	21	2	0
Luxembourg	61	31	42	19	34	15	16	2	2
Pays-Bas	39	23	35	18	37	15	30	2	1
Portugal	54	30	46	29	24	18	13	0	0
Espagne	61	32	29	31	41	8	9	0	2
Suède	47	17	38	17	40	11	26	0	1
Royaume-Uni	58	29	34	24	37	19	24	1	1
<b>UE15</b>	<b>48</b>	<b>27</b>	<b>36</b>	<b>23</b>	<b>38</b>	<b>16</b>	<b>23</b>	<b>1</b>	<b>1</b>

Note : cette question a été posée aux 16 % d'interviewés citoyens de l'UE qui avaient utilisé Internet pour faire des achats.

Source : Commission européenne, sondage Eurobaromètre spécial intitulé *European Union public opinion on issues relating to business to consumer e-commerce* (réf. : 201 EB60.0), mars 2004.

Tableau 3. Connaissance des labels de confiance Internet dans les pays de l'UE, 2003 (%)

	Oui	Non	NSP
Autriche	19	76	5
Belgique	9	86	5
Danemark	16	83	1
Finlande	11	82	7
France	9	89	3
Allemagne	15	77	9
Grèce	7	85	9
Irlande	10	86	4
Italie	6	90	4
Luxembourg	13	84	2
Pays-Bas	14	80	6
Portugal	6	92	2
Espagne	7	85	9
Suède	8	86	6
Royaume-Uni	8	88	4
<b>UE15</b>	<b>10</b>	<b>85</b>	<b>6</b>

Note : dans le contexte d'Internet, avez-vous entendu parler des labels de confiance Internet ? Cette question a été posée à tous les interviewés.

Source : Commission européenne, sondage Eurobaromètre spécial intitulé *European Union public opinion on issues relating to business to consumer e-commerce* (réf. : 201 EB60.0), mars 2004.

Tableau 4. Connaissance des mesures de sécurisation des données de paiement dans les pays de l'UE, 2003 (%)

	Oui	Non	NSP
Autriche	17	74	9
Belgique	13	81	6
Danemark	30	68	2
Finlande	22	70	8
France	24	73	3
Allemagne	21	69	9
Grèce	6	86	9
Irlande	18	77	5
Italie	18	76	6
Luxembourg	22	75	4
Pays-Bas	33	59	8
Portugal	10	88	2
Espagne	11	80	8
Suède	32	61	8
Royaume-Uni	27	70	4
<b>UE15</b>	<b>21</b>	<b>73</b>	<b>6</b>

*Note* : dans le contexte d'Internet, avez-vous entendu parler de notices sur la sécurité des données de paiement ? Cette question a été posée à tous les interviewés.

*Source* : Commission européenne, sondage Eurobaromètre spécial intitulé *European Union public opinion on issues relating to business to consumer e-commerce* (réf. : 201 EB60.0), mars 2004.

Tableau 5. Connaissance des mesures de protection des données personnelles dans les pays de l'UE, 2003 (%)

	Oui	Non	NSP
Autriche	25	68	7
Belgique	14	80	6
Danemark	32	66	2
Finlande	24	68	8
France	20	77	4
Allemagne	25	66	9
Grèce	9	82	9
Irlande	21	75	4
Italie	29	67	4
Luxembourg	26	72	3
Pays-Bas	38	56	6
Portugal	12	86	2
Espagne	16	76	8
Suède	33	59	8
Royaume-Uni	28	68	4
<b>UE15</b>	<b>24</b>	<b>70</b>	<b>6</b>

*Note* : dans le contexte d'Internet, avez-vous entendu parler de notices de protection des données personnelles ? Cette question a été posée à tous les interviewés.

*Source* : Commission européenne, sondage Eurobaromètre spécial intitulé *European Union public opinion on issues relating to business to consumer e-commerce* (réf. : 201 EB60.0), mars 2004.

Tableau 6. **Inquiétudes des internautes américains, 2000 (%)**

	Inquiet(ète)	Pas inquiet(ète)
Des entreprises et des gens que vous ne connaissez pas obtiennent sur vous et votre famille des renseignements personnels	84	15
Des pirates informatiques peuvent capter votre numéro de carte de crédit en ligne	68	30
Des personnes non qualifiées peuvent vous donner des renseignements médicaux en ligne	54	43
Avec des informations, vous téléchargez un virus informatique	54	45
Vous accédez en ligne à des actualités fausses ou imprécises	49	49
Des gens diffusent de fausses rumeurs en ligne pour peser sur les cours boursiers	47	50
Des gens que vous rencontrez en ligne mentent sur leur identité réelle	39	48
Quelqu'un pourrait savoir quels sites Internet vous avez consultés	31	68
Le message électronique que vous envoyez ne sera pas lu que par son destinataire	27	72

Source : *Pew Internet & American Life Project*, sondage de mai-juin 2000.

Tableau 7. **Inquiétudes des internautes américains, 1998 et 2000 (%)**

	1998	2000
Le message électronique que vous envoyez ne sera pas lu que par son destinataire	20	27
Quelqu'un pourrait savoir quels sites Internet vous avez consultés	21	31
Avec des informations, vous téléchargez un virus informatique	42	54

Source : *Pew Internet & American Life Project*, sondage de mai-juin 2000 et *The Pew Research Center for the People and the Press*, 1998.

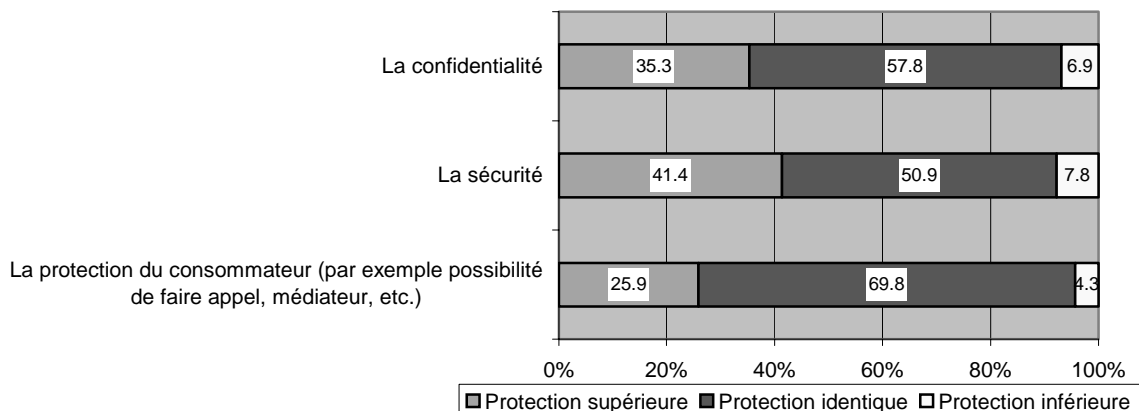
Tableau 8. **Conscience des internautes américains d'être suivis à la trace, 2000 (%)**

	Sait ce que c'est qu'un "mouchard"	Refuse les "mouchards"
Tous les internautes	43	10
Les internautes qui ont cliqué sur une annonce publicitaire	51	12
Les internautes qui ont acheté en ligne	56	11

Source : *Pew Internet & American Life Project*, sondage de mai-juin 2000.

Figure 1. Résultats de l'enquête de l'OCDE sur l'administration électronique, Danemark

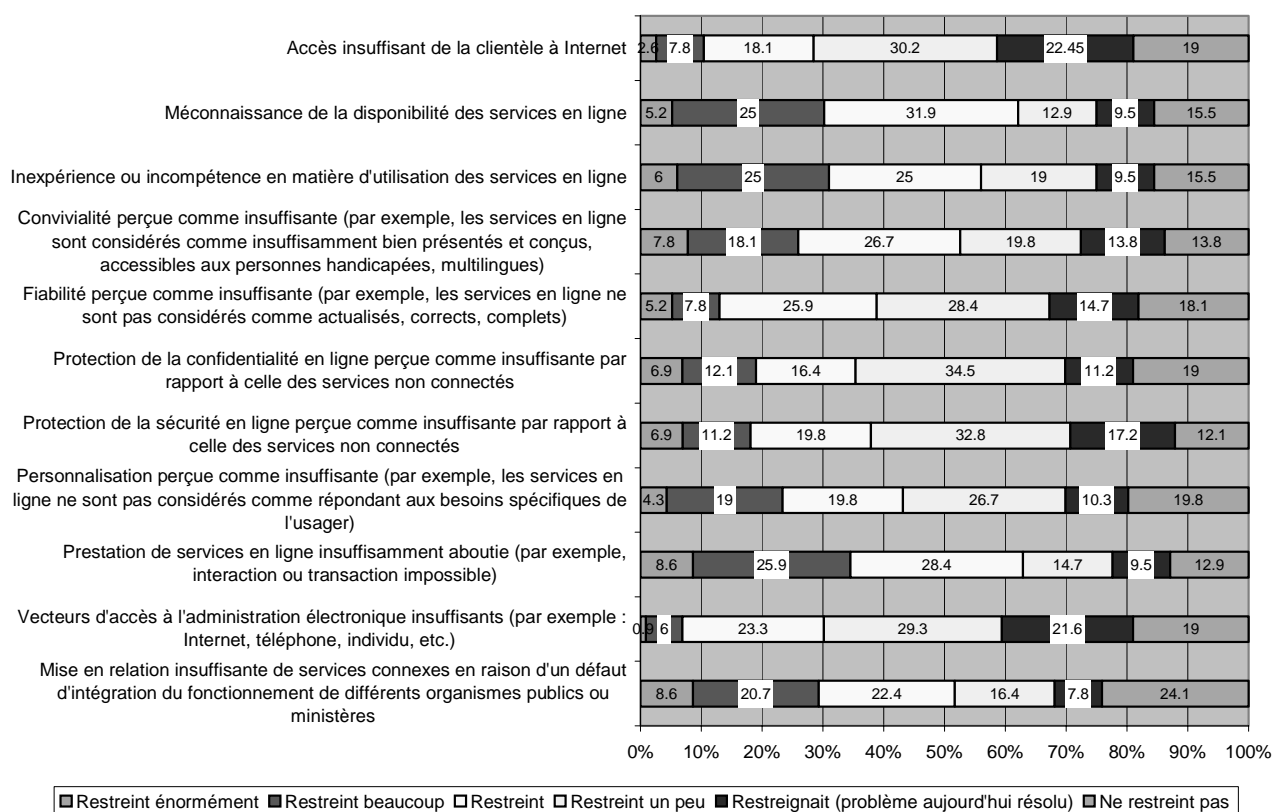
Q 3.5 Pensez-vous que les processus Internet de votre organisation présentent le même degré de protection que ses processus non connectés en ce qui concerne :



Source : Enquête GOV de l'OCDE sur l'administration électronique.

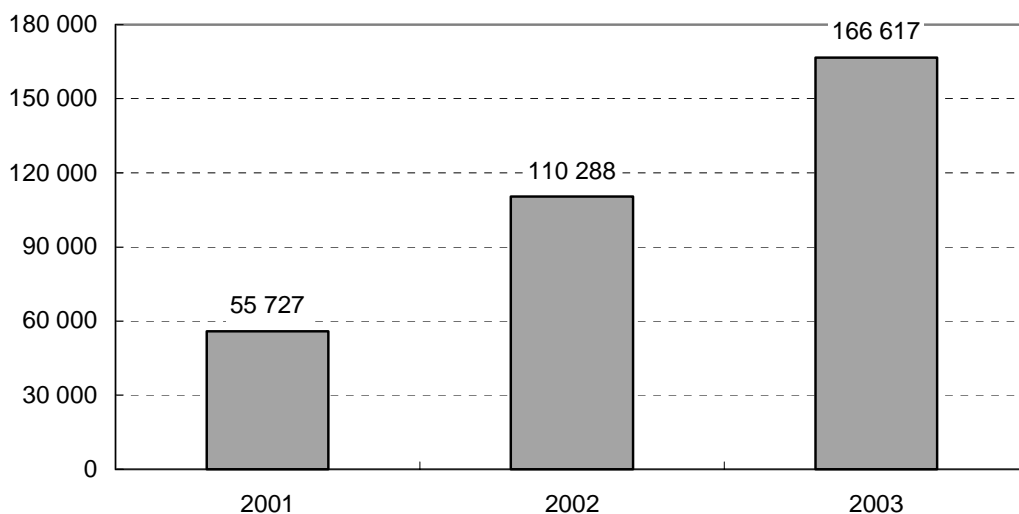
Figure 2. Résultats de l'enquête de l'OCDE sur l'administration électronique, Danemark

Q 7.4 Les éléments suivants restreignent-ils la demande, exprimée par la clientèle, de services en ligne fournis par votre organisation et, dans l'affirmative, à quel point ?



Source : Enquête GOV de l'OCDE sur l'administration électronique.

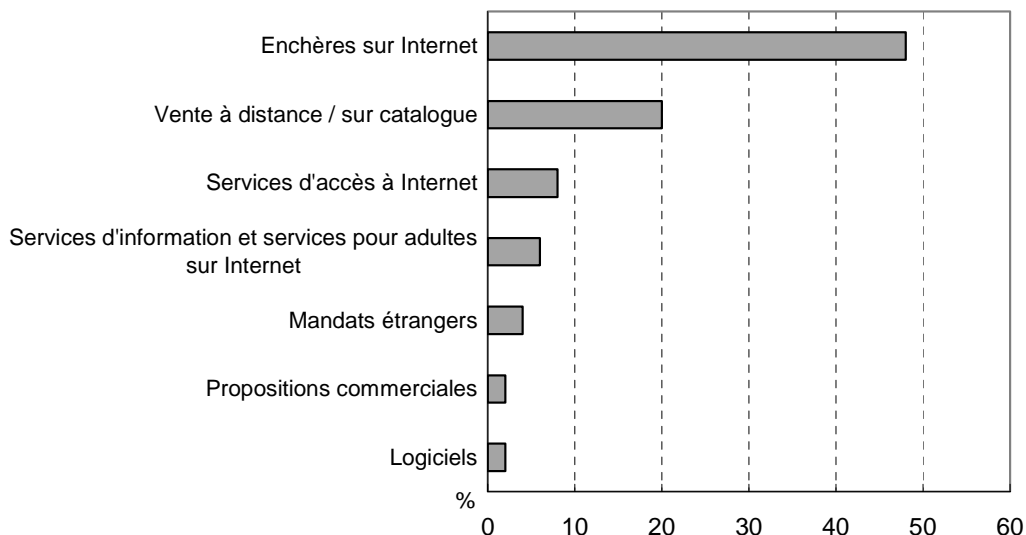
Figure 3. *Consumer Sentinel*, plaintes pour fraude concernant Internet, 2001-2003



1. Les données *Consumer Sentinel* couvrent l'ensemble des plaintes pour fraude relevées à l'échelle internationale.

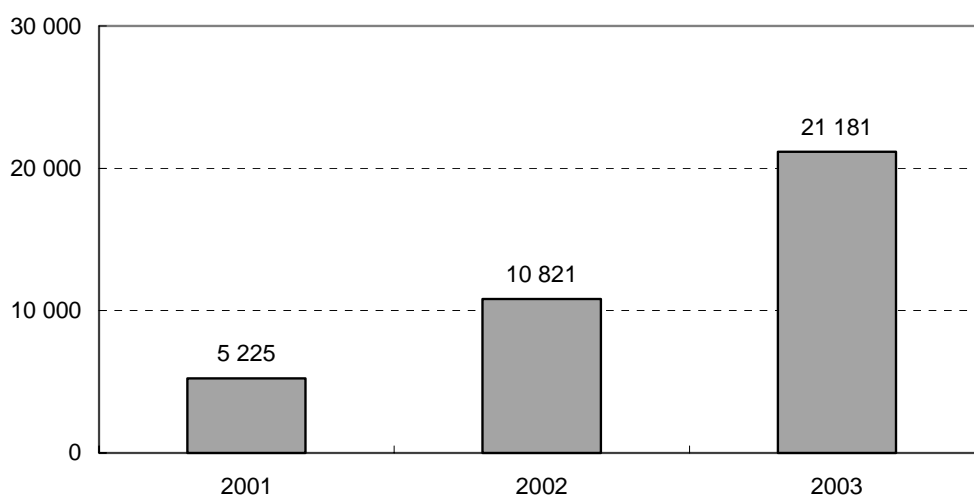
Source : FTC, [http://www.consumer.gov/sentinel/states03/3year\\_trends.pdf](http://www.consumer.gov/sentinel/states03/3year_trends.pdf), 13 septembre 2004.

Figure 4. *Consumer Sentinel*, produits ou services les plus concernés par les plaintes pour fraude concernant Internet<sup>1</sup>  
1<sup>er</sup> janvier–31 décembre 2003



1. Les pourcentages sont calculés à partir de l'ensemble des plaintes concernant Internet (166 617) reçues entre le 1<sup>er</sup> janvier et le 31 décembre 2003.

Source : FTC, [http://www.consumer.gov/sentinel/states03/internet\\_related\\_trends.pdf](http://www.consumer.gov/sentinel/states03/internet_related_trends.pdf), 13 septembre 2004.

Figure 5. *Consumer Sentinel*, plaintes transfrontières pour fraude concernant Internet, 2001-2003

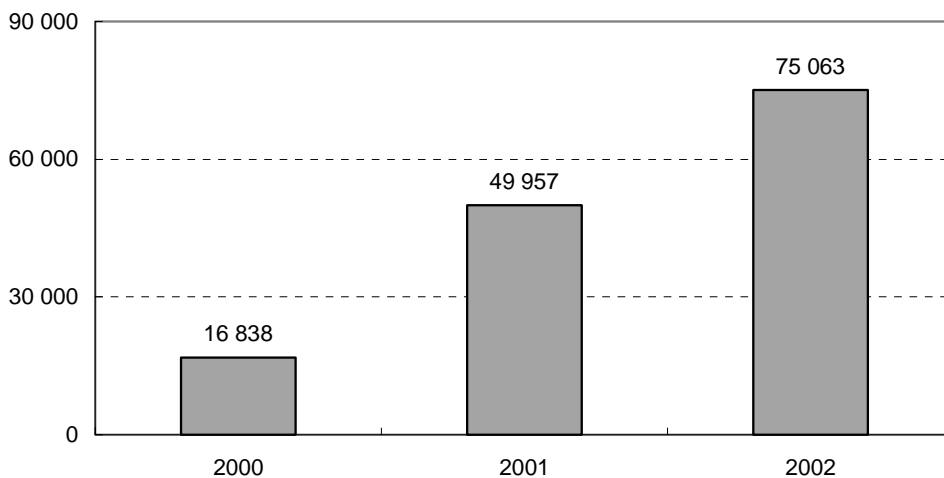
Source : FTC, <http://www.ftc.gov/opa/2004/03/cbcy2003.pdf>, 15 septembre 2004.

Tableau 9. *Consumer Sentinel*, principaux lieux des plaintes de consommateurs et d'entreprises, 1er janvier-30 juin 2004

Principaux lieux des plaintes de consommateurs		Principaux lieux des plaintes d'entreprises	
États-Unis	2 774	États-Unis	791
Royaume-Uni	138	Royaume-Uni	449
Canada	109	Pays-Bas	184
Australie	105	Canada	174
France	27	Espagne	147
Nouvelle-Zélande	22	Nigeria	130
Inde	21	Afrique du Sud	75
Suède	17	Australie	72
Belgique	15	Italie	64
Allemagne	15	Allemagne	63

Source : FTC, <http://www.econsumer.gov/english/contentfiles/pdfs/PU15%20-%20Jan-Jun%202004.pdf>, 15 septembre 2004.

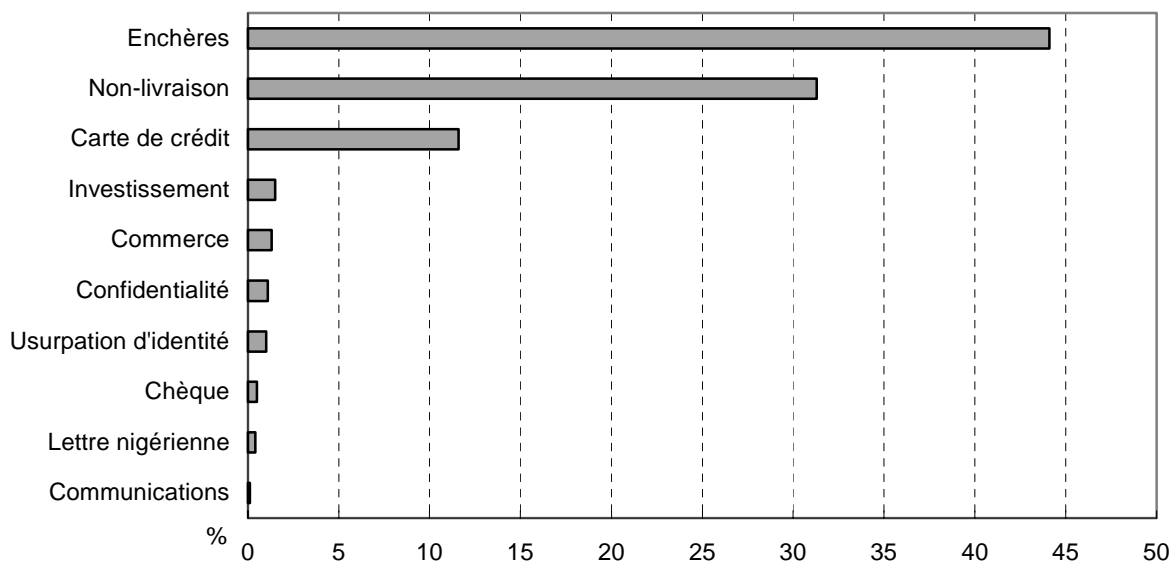
Figure 6. **IFCC, plaintes pour fraude concernant Internet, 2000-2002**



1. Les données IFCC concernent les États-Unis.

Source : [http://www.ifccfbi.gov/strategy/2002\\_IFCCReport.pdf](http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf), 15 septembre 2004.

Figure 7. **IFCC, principaux motifs des plaintes pour fraude concernant Internet<sup>1</sup>**  
1<sup>er</sup> janvier-31 décembre 2002



1. Les pourcentages sont calculés à partir de l'ensemble des plaintes concernant Internet (75 063) reçues entre le 1<sup>er</sup> janvier et le 31 décembre 2002.

Source : IFCC, [http://www.consumer.gov/sentinel/states03/internet\\_related\\_trends.pdf](http://www.consumer.gov/sentinel/states03/internet_related_trends.pdf), 13 septembre 2004.

Tableau 10. **Pays hôte des sites de *phishing***  
**[tentative d'escroquerie par usurpation de l'identité d'un site]**

	Ensemble des sites de <i>phishing</i> (%), juin 2004	Ensemble des sites de <i>phishing</i> (%), décembre 2004
États-Unis	27	32
Corée (du Sud)	20	11
Chine	16	12
Taipei chinois	7	
Pays-Bas	3	
Mexique	2	
Uruguay	2	
Turquie	2	
Brésil	1	2.7
Croatie	1	
Royaume-Uni	1	
Thaïlande	1	
Portugal	1	
Pologne	1	
Suède	1	
Madagascar	1	
Russie	1	
Espagne	1	
Pays indétectable	10	
Japon		2.8
Allemagne		2.7
France		2.7
Roumanie		2.2
Canada		2.1
Inde		2.1

Source : Anti Phishing Working Group.

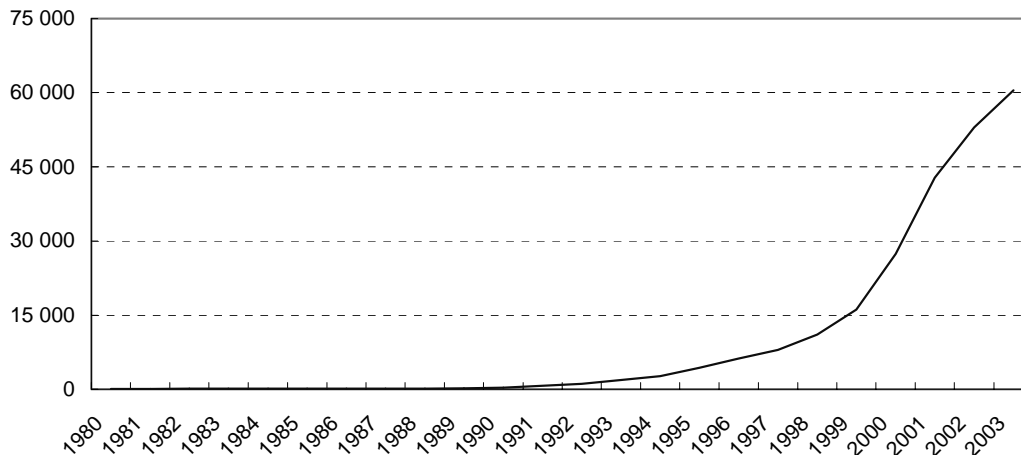
Tableau 11. Sites de *phishing* par pays enregistrés par la barre d'outils Netcraft

Pays	Code TLD (domaines nationaux)	Nombre total de sites	Sites de <i>phishing</i>	Pourcentage de sites de <i>phishing</i> connus	Probabilité de présence de sites de <i>phishing</i> (1)
Syrie	SY	58	4	0.1	1 sur 14
Cameroun	CM	49	1	0.0	1 sur 49
Îles Marianne du Nord	MP	153	1	0.0	1 sur 153
Brunéi Darussalam	BN	302	1	0.0	1 sur 302
Jamaïque	JM	328	1	0.0	1 sur 328
Pakistan	PK	4 035	10	0.2	1 sur 403
Taipei chinois	TW	79 823	188	4.2	1 sur 424
Philippines	PH	8 250	18	0.4	1 sur 458
Arménie	AM	541	1	0.0	1 sur 541
Viet Nam	VN	2 481	4	0.1	1 sur 620
Honduras	HN	639	1	0.0	1 sur 639
Roumanie	RO	41 772	65	1.5	1 sur 642
Bélarus	BY	1 944	3	0.1	1 sur 648
Namibie	NA	696	1	0.0	1 sur 696
Iran	IR	4 338	6	0.1	1 sur 723
Bolivie	BO	1 820	2	0.0	1 sur 910
Mongolie	MN	952	1	0.0	1 sur 952
Nicaragua	NI	962	1	0.0	1 sur 962
Territoires palestiniens	PS	977	1	0.0	1 sur 977
Équateur	EC	2 957	3	0.1	1 sur 985
Paraguay	PY	1 988	2	0.0	1 sur 994
Colombie	CO	10 864	10	0.2	1 sur 1 086
Bahamas	BS	1 164	1	0.0	1 sur 1 164
Égypte	EG	8 705	7	0.2	1 sur 1 243
Fédération de Russie	RU	299 078	168	3.7	1 sur 1 780
Lituanie	LT	12 558	7	0.2	1 sur 1 794
Inde	SUR	102 659	54	1.2	1 sur 1 901
Sri Lanka	LK	1 941	1	0.0	1 sur 1 941
Maroc	MA	7 931	4	0.1	1 sur 1 982
Guatemala	GT	2 078	1	0.0	1 sur 2 078
Malaisie	MY	48 384	23	0.5	1 sur 2 103
Corée	KR	1 026 567	486	10.8	1 sur 2 112
Costa Rica	CR	6 525	3	0.1	1 sur 2 175
Kenya	KE	2 207	1	0.0	1 sur 2 207
Brésil	BR	219 287	98	2.2	1 sur 2 237
Porto Rico	PR	2 290	1	0.0	1 sur 2 290
Indonésie	ID	24 220	10	0.2	1 sur 2 422
Pérou	PE	4 877	2	0.0	1 sur 2 438
Thaïlande	TH	64 264	26	0.6	1 sur 2 471
Argentine	AR	161 173	59	1.3	1 sur 2 731
Hong Kong, Chine	HK	146 847	53	1.2	1 sur 2 770
Chili	CL	70 499	23	0.5	1 sur 3 065
Chine	CN	1 159 391	350	7.8	1 sur 3 312
Panama	PA	3 371	1	0.0	1 sur 3 371
Mexique	MX	59 926	14	0.3	1 sur 4 280
Bulgarie	BG	39 542	7	0.2	1 sur 5 648
Islande	IS	12 486	2	0.0	1 sur 6 243
Uruguay	UY	19 385	3	0.1	1 sur 6 461
Turquie	TR	160 215	24	0.5	1 sur 6 675
Pologne	PL	248 603	34	0.8	1 sur 7 311

1. Classement Netcraft.

Source : Netcraft (5 avril 2005).

Figure 8. **Les espioniciels en chiffres**  
Décompte annuel de l'ensemble des logiciels parasites, 1980–2003<sup>1</sup>



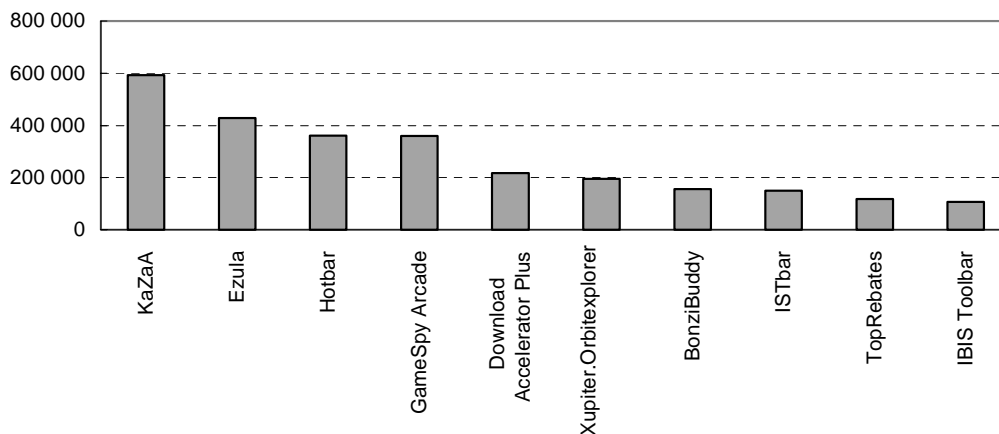
1. Dernière révision du samedi 13 décembre 2003.

Ce graphique fournit le cumul des logiciels parasites recensés dans la catégorie « Tous logiciels parasites ». Le chiffre annuel représente le volume approximatif de programmes de ce type recensés l'année en question. Notez que ces chiffres peuvent constituer des sous-estimations, en particulier pour les nouveaux logiciels parasites de ces dernières années, car ceux-ci ont parfois moins de chances de dominer ou de figurer dans des catégories définies.

Les volumes sont cumulés d'année en année car les chevaux de Troie et autres logiciels parasites ne « disparaissent » jamais, même si, bien entendu, la probabilité de les rencontrer peut évoluer.

Source : [http://research.pestpatrol.com/Trends/All\\_Pests\\_Counts\\_by\\_Year.asp](http://research.pestpatrol.com/Trends/All_Pests_Counts_by_Year.asp), 5 octobre 2004.

Figure 9. **Les 10 logiciels parasites les plus actifs dans les 28 derniers jours**<sup>1</sup>

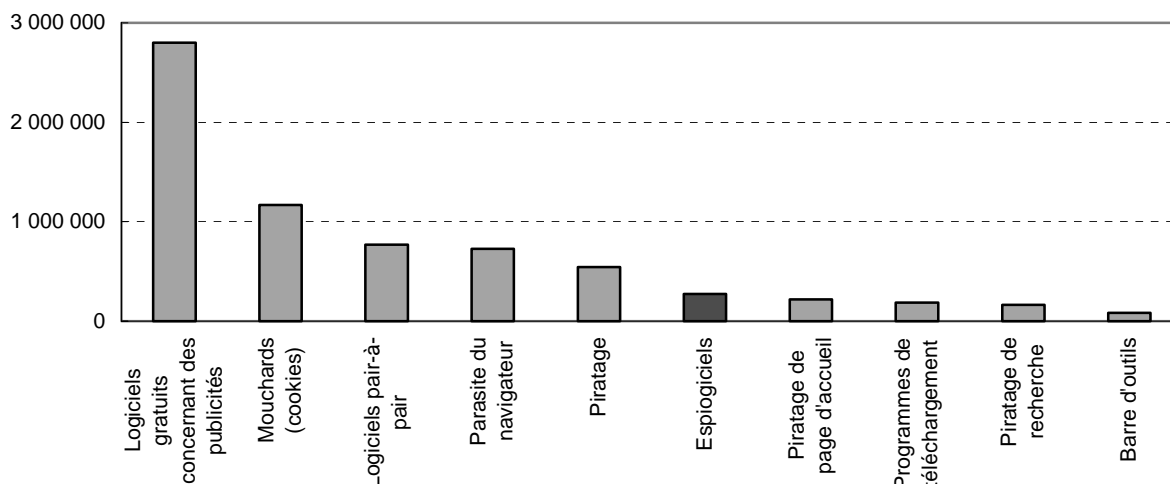


1. Dernière mise à jour le mardi 5 octobre 2004.

Ce graphique résume les dix premiers logiciels parasites, qui représentent 2 688 751 signalements de programmes parasites sur les 6 618 454 signalements effectués par les utilisateurs PestPatrol au cours des 28 derniers jours. Dans ces tableaux, chaque rapport est un « objet » unique tel qu'une entrée de registre, un fichier ou un répertoire. Au total, 1 996 types distincts de logiciels parasites ont été signalés.

Source : <http://research.pestpatrol.com/Lists/MostPrevalentPests.asp>, 5 octobre 2004.

Figure 10. Les 10 premiers types de logiciels parasites dans les 28 derniers jours<sup>1</sup>

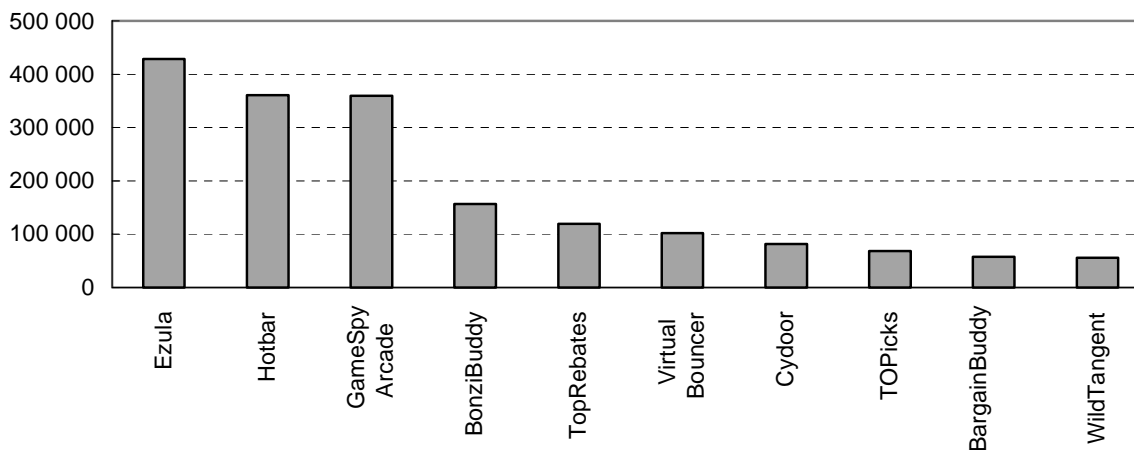


1. Dernière mise à jour le mardi 5 octobre 2004.

Ce graphique résume, par catégorie, 6 937 456 des 7 153 591 signalements de logiciels parasites effectués au total par les utilisateurs PestPatrol au cours des 28 derniers jours. Dans ces tableaux, chaque rapport est un « objet » unique tel qu'une entrée de registre, un fichier ou un répertoire. Au total, 2 253 types distincts de logiciels parasites ont été signalés.

Source : <http://research.pestpatrol.com/Lists/MostPrevalentPests.asp>, 5 octobre 2004.

Figure 11. Les 10 premiers espiociels éliminés dans les 28 derniers jours<sup>1</sup>



1. Dernière mise à jour le mardi 5 octobre 2004.

Ce tableau est tiré des 6 546 623 signalements de logiciels parasites effectués au total par les utilisateurs de PestPatrol au cours du mois écoulé. Ce graphique reprend les logiciels parasites les plus courants dans la catégorie « Tous espiociels (comprend les *trackware* [logiciels qui enregistrent les habitudes de l'utilisateur et transmettent ces informations à des tiers] et les publiciels [*adware*], mais pas les mouchards [*cookies*] des espiociels) »

Source : <http://research.pestpatrol.com/Lists/TopTenPestsByType.asp>, 5 octobre 2004.

Tableau 12. **Ordinateurs infectés par un bot, par pays (juillet-décembre 2004)**

Pays	Ordinateurs infectés par un <i>bot</i> (pourcentage de l'ensemble)
Royaume-Uni	25.2
États-Unis	24.6
Chine	7.8
Canada	4.9
Espagne	3.8
France	3.6
Allemagne	3.5
Taipei chinois	3.1
Corée	3.0
Japon	2.6
Reste du monde	17.9

Source : Symantec Internet Security Threat Report (publié en mars 2005).

Tableau 13. Ordinateurs infectés par un *bot*, par pays (juillet-décembre 2004)

Pays	Ordinateurs infectés par un <i>bot</i> (juillet-décembre 2004)	Ordinateurs infectés par un <i>bot</i> , pour 10 000 habitants	Ordinateurs infectés par un <i>bot</i> , pour 100 abonnés au haut débit (1)	Proportion d'abonnés au haut débit - OCDE (septembre 2004) (%)	Proportion d'ordinateurs infectés par un <i>bot</i> - OCDE (%)
Australie	9 650	4.8	0.74	1.23	1.29
Autriche	4 235	5.2	0.57	0.70	0.57
Belgique	3 469	3.3	0.22	1.46	0.47
Canada	43 609	13.8	0.81	5.03	5.85
République tchèque	884	0.9	0.65	0.13	0.12
Danemark	6 855	12.7	0.72	0.90	0.92
Finlande	4 091	7.8	0.64	0.60	0.55
France	31 874	5.2	0.58	5.16	4.28
Allemagne	31 035	3.8	0.53	5.54	4.16
Grèce	574	0.5	1.77	0.03	0.08
Hongrie	1 682	1.7	0.57	0.28	0.23
Islande	337	11.6	0.72	0.04	0.05
Irlande	466	1.2	0.48	0.09	0.06
Italie	19 092	3.3	0.49	3.66	2.56
Japon	22 712	1.8	0.13	16.21	3.05
Corée	26 660	5.6	0.23	11.07	3.58
Luxembourg	186	4.1	0.54	0.03	0.02
Mexique	2 578	0.3	0.40	0.61	0.35
Pays-Bas	7 635	4.7	0.26	2.70	1.02
Nouvelle-Zélande	647	1.6	0.40	0.15	0.09
Norvège	3 696	8.1	0.66	0.53	0.50
Pologne	7 411	1.9	1.01	0.69	0.99
Portugal	17 205	16.5	2.30	0.70	2.31
République slovaque	224	0.4	0.52	0.04	0.03
Espagne	34 076	8.4	1.18	2.71	4.57
Suède	13 172	14.7	1.11	1.11	1.77
Suisse	6 724	9.1	0.58	1.09	0.90
Turquie	1 691	0.2	0.69	0.23	0.23
Royaume-Uni	223 836	37.7	4.25	4.95	30.04
États-Unis	218 911	7.5	0.64	32.32	29.38
OCDE	745 217	6.5	0.70	100.00	100.00

1. Dans la pratique, certains ordinateurs se connectant à l'aide d'une ligne téléphonique seraient aussi infectés. Cet indicateur n'a pas pour ambition de prendre ce fait en compte ; il s'agit simplement du nombre d'ordinateurs infectés par un programme *bot* (ce qui engloberait les ordinateurs connectés *via* une ligne téléphonique) rapporté au nombre d'abonnés au haut débit.

Source : Symantec, OCDE.

Tableau 14. Répartition du marché de la certification SSL (juillet 2004)

Entreprise	Part de marché (%)
Verisign (dont Thawte)	39
RSA Security (dont les certificats Verisign)	22
Geotrust	19
Comodo	11
Autres	9
Total	100

Source : OCDE, d'après des enquêtes Netcraft ([www.netcraft.com](http://www.netcraft.com)).

Tableau 15. **Serveurs sécurisés dans la zone OCDE**

	Serveurs sécurisés juillet 1998	Serveurs sécurisés juillet 1999	Serveurs sécurisés juillet 2000	Serveurs sécurisés juillet 2001	Serveurs sécurisés juillet 2002	Serveurs sécurisés juillet 2003	Serveurs sécurisés juillet 2004	Pour 100 000 habitants (juillet 1998)	Pour 100 000 habitants (juillet 1999)	Pour 100 000 habitants (juillet 2000)	Pour 100 000 habitants (juillet 2001)	Pour 100 000 habitants (juillet 2002)	Pour 100 000 habitants (juillet 2003)	Pour 100 000 habitants (juillet 2004)
Australie	632	1 305	2 828	3 704	4 693	4 830	8 079	3.4	6.9	14.7	19.0	23.8	24.5	40.9
Autriche	98	241	447	881	949	1 073	1 590	1.2	3.0	5.6	11.0	11.8	13.3	19.7
Belgique	52	159	268	431	439	512	912	0.5	1.6	2.6	4.2	4.2	5.0	8.8
Canada	929	1 789	3 896	6 050	7 768	9 378	15 166	3.1	5.9	12.7	19.4	24.7	29.9	48.3
République tchèque	19	88	194	383	185	213	315	0.2	0.9	1.9	3.7	1.8	2.1	3.1
Danemark	44	112	289	523	660	890	1 681	0.8	2.1	5.4	9.8	12.3	16.5	31.2
Finlande	68	180	343	660	744	870	1 255	1.3	3.5	6.6	12.7	14.3	16.7	24.1
France	222	632	1 297	1 969	2 511	2 646	3 799	0.4	1.0	2.1	3.2	4.1	4.3	6.2
Allemagne	492	1 630	3 761	6 442	7 987	7 912	13 163	0.6	2.0	4.6	7.8	9.7	9.6	16.0
Grèce	8	48	87	176	170	181	270	0.1	0.4	0.8	1.6	1.6	1.7	2.5
Hongrie	18	26	90	165	86	122	199	0.2	0.3	0.9	1.6	0.8	1.2	2.0
Islande	13	29	67	91	136	170	249	4.7	10.5	23.8	31.9	47.3	59.1	86.6
Irlande	56	97	245	467	579	701	1 201	1.5	2.6	6.4	12.1	14.8	17.9	30.7
Italie	167	432	795	1 264	1 167	1 327	1 977	0.3	0.7	1.4	2.2	2.0	2.3	3.4
Japon	429	1 170	2 900	7 952	7 179	10 513	19 610	0.3	0.9	2.3	6.2	5.6	8.2	15.4
Corée	38	106	243	397	562	623	878	0.1	0.2	0.5	0.8	1.2	1.3	1.8
Luxembourg	11	26	44	68	97	104	184	2.6	6.0	10.0	15.4	21.7	23.3	41.2
Mexique	26	58	176	310	324	379	605	0.0	0.1	0.2	0.3	0.3	0.4	0.6
Pays-Bas	127	306	541	1 064	1 332	1 723	3 595	0.8	1.9	3.4	6.6	8.2	10.7	22.3
Nlle-Zélande	90	227	482	778	983	1 124	1 668	2.4	5.9	12.4	19.9	24.7	28.3	42.0
Norvège	55	130	273	491	528	666	1 122	1.2	2.9	6.1	10.9	11.6	14.7	24.7
Pologne	23	61	188	467	373	382	557	0.1	0.2	0.5	1.2	1.0	1.0	1.5
Portugal	27	59	116	192	214	286	443	0.3	0.6	1.1	1.9	2.1	2.8	4.3
Rép. slovaque	15	..	45	110	38	47	61	0.3	..	0.8	2.0	0.7	0.9	1.1
Espagne	239	432	759	1 194	1 315	1 764	2 745	0.6	1.1	1.9	3.0	3.2	4.4	6.8
Suède	145	406	811	1 261	1 246	1 437	2 826	1.6	4.6	9.1	14.2	14.0	16.1	31.7
Suisse	152	401	854	1 370	1 555	1 769	2 826	2.1	5.6	11.8	18.9	21.2	24.1	38.5
Turquie	7	50	116	285	400	432	855	0.0	0.1	0.2	0.4	0.6	0.6	1.2
Royaume-Uni	714	1 735	4 404	7 916	10 288	11 714	20 339	1.2	3.0	7.5	13.4	17.4	19.8	34.4
États-Unis	14 674	32 053	65 565	86 025	106 884	120 661	197 769	5.3	11.5	23.2	30.2	37.2	42.0	68.8
OCDE	19 590	43 988	92 124	133 086	161 392	184 449	305 939	1.8	3.9	8.2	11.7	14.1	16.1	26.7

Source : OCDE, d'après des enquêtes Netcraft ([www.netcraft.com](http://www.netcraft.com)).

## NOTES

1. Le Groupe de travail sur la sécurité de l'information et de la vie privée (GTSIVP) de l'OCDE oeuvre pour une approche internationale coordonnée de l'action publique en matière de sécurité et de protection de la vie privée et des données de caractère personnel afin de contribuer à renforcer la confiance. L'expression « confiance dans l'environnement en ligne » est ici utilisée pour couvrir un certain nombre d'aspects liés à la confiance, notamment la sécurité de l'environnement et des informations placées dans cet environnement, la protection de la vie privée et d'autres questions de confiance comme la protection des consommateurs et les problèmes liés à des aspects de l'environnement en ligne tels que l'existence de sites Web perçus comme préjudiciables (par exemple aux enfants).
2. OCDE, « Indicateurs clés des TIC », [http://www.oecd.org/document/23/0,2340,en\\_2649\\_34225\\_33987543\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/23/0,2340,en_2649_34225_33987543_1_1_1_1,00.html).
3. Voir <http://www.whitehouse.gov/omb/memoranda/m03-19.pdf>.
4. Voir <http://www.gao.gov/highlights/d04483thigh.pdf>.
5. Voir par exemple Jonathan Cave, « The Economics of Trust Between Cyber Partners », [http://www.foresight.gov.uk/previous\\_projects/cyber\\_trust\\_and\\_crime\\_prevention/reports\\_and\\_publication\\_s/index.html](http://www.foresight.gov.uk/previous_projects/cyber_trust_and_crime_prevention/reports_and_publication_s/index.html) et les communications au quatrième atelier sur l'économie de la sécurité de l'information, Kennedy School of Government, Université Harvard, 2-3 juin 2005 : <http://infoecon.net/workshop/schedule.php>.
6. Pour les questionnaires et des informations générales sur l'enquête, voir : <http://www.census.gov/eos/www/css/css.html>.
7. [http://europa.eu.int/comm/public\\_opinion/index\\_en.htm](http://europa.eu.int/comm/public_opinion/index_en.htm).
8. [http://europa.eu.int/comm/consumers/topics/btoc\\_ecomm.pdf](http://europa.eu.int/comm/consumers/topics/btoc_ecomm.pdf). Cette étude a comporté des entretiens en face à face avec 16 205 citoyens des 15 pays de l'UE.
9. Commission européenne, « Protection des données », Eurobaromètre spécial, décembre 2003. [http://europa.eu.int/comm/public\\_opinion/archives/ebs/ebs\\_196\\_highlights.pdf](http://europa.eu.int/comm/public_opinion/archives/ebs/ebs_196_highlights.pdf).
10. Verisign, « Enhanced VeriSign Secured™ Seal Enables Consumers to Verify E-Commerce Site Security Prior to Transacting Business Online », Communiqué de presse, 2 novembre 2004. [http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2004/page\\_017440.html](http://www.verisign.com/verisign-inc/news-and-events/news-archive/us-news-2004/page_017440.html).
11. L'échantillon en ligne était constitué de 2 237 adultes originaires de toutes les régions du pays et comprenait 1 073 hommes et 1 164 femmes, âgés de 18 ans et plus. L'échantillon en ligne des personnes ayant effectué un achat en ligne à une période quelconque de leur vie était constitué de 2 027 adultes choisis dans tout le pays, dont 987 hommes et 1 040 femmes âgés de 18 ans et plus.
12. Susan Kuchinskas, « VeriSign Strengthens Secured Seal », 17 novembre 2004. <http://www.ecommerce-guide.com/essentials/paypal/article.php/3436811>.
13. Verisign, « Enhanced VeriSign Secured™ Seal Enables Consumers to Verify E-Commerce Site Security Prior to Transacting Business Online », Op cit.

14. AOL/NCSA Online Safety Study, octobre 2004.  
[http://www.staysafeonline.info/news/safety\\_study\\_v04.pdf](http://www.staysafeonline.info/news/safety_study_v04.pdf).
15. Dr. Malte Krueger et Kay Leibold, « Internet Payment Systems: The Consumers' View », Karlsruhe, novembre 2004.
16. George Danezis, Stephen Lewis et Ross Anderson, « How much is privacy location worth », document daté de février 2005 devant être présenté au quatrième atelier sur l'économie de la sécurité de l'information, Kennedy School of Government, Harvard University, 2-3 juin 2005.  
<http://infoecon.net/workshop/pdf/38.pdf>.
17. Par exemple : Nielsen/NetRatings, « Over 18 million Europeans bank online, but they trust traditional banking brands on the Internet », communiqué de presse, 20 novembre 2002.
18. Rob O'Neill, « Banks wary of online monitoring », *The Age*, 22 mars 2005.  
<http://www.theage.com.au/articles/2005/03/21/1111253920118.html>.
19. [http://www.pewinternet.org/pdfs/PIP\\_Trust\\_Privacy\\_Report.pdf](http://www.pewinternet.org/pdfs/PIP_Trust_Privacy_Report.pdf). Entre mai et juin 2000, le *Pew Internet & American Life Project* a interrogé 2 117 Américains adultes (âgés de plus de 18 ans), dont 1 017 internautes. Les entretiens ont été conduits par téléphone.
20. *Consumer Reports*, « Net Threat Rising », (daté de septembre 2005), <http://www.consumerreports.org>.
21. [http://i.cmpnet.com/gocsi/db\\_area/pdfs/fbi/FBI2004.pdf](http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf).
22. <http://www.csoonline.com/releases/ecrimewatch04.pdf>.
23. AusCERT, « Computer Crime and Security Survey », 2004.  
<http://www.auscert.org.au/render.html?it=2001>.
24. Voir par exemple pour l'enquête 2002 :  
[http://www.btglobalservices.com/en/products/trustservices/docs/security\\_breaches\\_2002.pdf](http://www.btglobalservices.com/en/products/trustservices/docs/security_breaches_2002.pdf).
25. Voir NHTCU, « High Tech Crime: The Impact on UK Business », 2004 :  
<http://www.nhtcu.org/NOP%20Survey.pdf>.
26. Bill Goodwin, « E-crime is costing UK business £2.4bn a year, says police report », *Computerweekly.com*, 5 avril 2005.  
<http://www.computerweekly.com/articles/article.asp?liArticleID=137740&liArticleTypeID=1&liCategoryID=6&liChannelID=22&liFlavourID=1&sSearch=&nPage=1>.
27. Voir : [www.vm.fi/tiedostot/pdf/fi/95054.pdf](http://www.vm.fi/tiedostot/pdf/fi/95054.pdf).
28. [www.asimelec.es](http://www.asimelec.es) L'étude est disponible à l'adresse suivante :  
<http://www.asimelec.es/pdf/seguridad/asimelec%20estudio%20mercado%20ISO17799-021024.pdf>.
29. « Survey Reveals that Consumers and Tech Professionals Share Concern About Cybercrime, But Only 19.5 Percent of Consumers And 48.9 Percent of Tech Professionals Currently Use a Personal Firewall », communiqué de presse, 29 juin 2004, <http://www.symantec.com/press/2000/n000629a.html>. Un pare-feu est un système conçu pour empêcher l'accès non autorisé en provenance ou à destination d'un réseau privé. Les pare-feu peuvent être logiciels ou matériels, ou combiner les deux types de protection. Voir : <http://www.webopedia.com/TERM/f/firewall.html>.

30. Sarah Gordon, « Privacy: A Study of Attitudes and Behaviours in the US, UK and EU Information Security Professionals », Symantec White Paper, 2004.  
<http://securityresponse.symantec.com/avcenter/reference/privacy.attitudes.behaviors.pdf>.
31. Deloitte, « 2004 Global Security Survey », 2004, <http://www.deloitte.com/dtt/cda/doc/content/GFSISE.pdf>
32. PLS RAMBOLL, « E-business Nordic.com 2003 », Aarhus, novembre 2003.
33. <http://www.consumer.gov/sentinel/> et <http://www.ftc.gov/>.
34. <http://www.ifccfbi.gov/>.
35. <http://www.ifccfbi.gov/strategy/statistics.asp>.
36. <http://www.fraud.org/internet/intinfo.htm>.
37. <http://www.fraud.org/2004-internet%20scams.pdf>.
38. <http://www.fraud.org/2003internetscams.pdf>.
39. <http://www.econsumer.gov/english/index.html>.
40. <http://www.icpen.org>.
41. <http://www.econsumer.gov/english/contentfiles/pdfs/PU15%20-%20Jan-Jun%202004.pdf>.
42. Symantec, « Internet Security Threat Report », Trends for 1 January–30 June, 2004, septembre 2004.  
[http://www.symantec.com/region/se/seresc/download/istr\\_sept\\_2004.pdf](http://www.symantec.com/region/se/seresc/download/istr_sept_2004.pdf).
43. <http://www.census.gov/mrts/www/current.html>.
44. Visa, « VISA EU 2003 Annual Results », communiqué de presse, avril 2004,  
[http://www.visaeu.com/pressandmedia/press188\\_pressreleases.html](http://www.visaeu.com/pressandmedia/press188_pressreleases.html).
45. APACS, « 10 per cent of all credit card payments now made on-line », communiqué de presse, 5 août 2004, <http://www.apacs.org.uk>.
46. Visa Quarterly Report, avril-juin 2004, <http://usa.visa.com/media/global/Q22004.pdf>.
47. Les taux globaux de fraude sont disponibles à l'adresse suivante :  
[http://usa.visa.com/personal/newsroom/fraud\\_security.html?it=il\\_/personal/site\\_map/visa\\_analyst\\_center.html](http://usa.visa.com/personal/newsroom/fraud_security.html?it=il_/personal/site_map/visa_analyst_center.html).
48. [http://www.mastercardintl.com/newsroom/programs\\_faqs.html#fraud](http://www.mastercardintl.com/newsroom/programs_faqs.html#fraud).
49. Susanne Schnorr-Bäcker, Bureau fédéral de statistiques, Allemagne, « Towards the knowledge society: ICT regarding households and individuals in Germany ». Communication présentée à la réunion thématique du SMSI sur la mesure de la société de l'information, Genève, 7-9 février 2005. Ces données ne portent que sur l'ancien territoire de la République fédérale, englobant l'ensemble de Berlin.
50. Il peut exister des délits liés à l'utilisation des TIC qui ne sont pas pris en compte dans ce système.
51. Schnorr-Bäcker, Op.cit.

52. Voir [http://www.usdoj.gov/opa/pr/2004/August/04\\_crm\\_583.htm](http://www.usdoj.gov/opa/pr/2004/August/04_crm_583.htm) consulté le 6 octobre 2004.
53. ACPR, Standardisation of Definitions of Identity Crime Terms, Discussion Paper, mai 2004, <http://www.acpr.gov.au/pdf/Standdefinit.pdf>.
54. Australian Bureau of Statistics, « Development of e-crime statistics », National Crime Statistics Unit, non publié, 21 septembre 2004.
55. <http://www.austrac.gov.au/policy/DEFINITIONSjoint.pdf>.
56. Federal Deposit Insurance Corporation (FDIC), « Putting an End to Account-Hijacking Identity Theft », 14 décembre 2004, [http://www.fdic.gov/consumers/consumer/idtheftstudy/identity\\_theft.pdf](http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf).
57. Home Office Identity Fraud Steering Committee, site Web, 28 février 2005, <http://www.identity-theft.org.uk/>.
58. Australian centre for Policing Research, « Identity Crime Research and Coordination », février 2005. [http://www.acpr.gov.au/research\\_idcrime.asp](http://www.acpr.gov.au/research_idcrime.asp) and Susan Cuganesan and David Lacey, *Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent*, CIRCA, septembre 2003. [http://www.austrac.gov.au/publications/identity\\_fraud/identity\\_fraud\\_extract.pdf](http://www.austrac.gov.au/publications/identity_fraud/identity_fraud_extract.pdf).
59. FDIC, Op.cit.
60. Voir <http://www.enisa.eu.int/> (octobre 2004).
61. [http://www.enisa.eu.int/about/activities/index\\_en.htm](http://www.enisa.eu.int/about/activities/index_en.htm).
62. <http://www.enisa.eu.int/>.
63. <http://www.waarschuwingsdienst.nl/render.html?cid=106>.
64. <http://www.itsafe.gov.uk/links/international.html>.
65. <http://www.ahtcc.gov.au/>.
66. <http://webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase>.
67. La définition de « Pharming » est extraite du site Web de l'Anti-Phishing Working Group à l'adresse : <http://www.antiphishing.org/>. Netcraft a signalé un incident d'empoisonnement de cache en mars 2005: [http://news.netcraft.com/archives/2005/03/07/dns\\_poisoning\\_scam\\_raises\\_wariness\\_of\\_pharming.html](http://news.netcraft.com/archives/2005/03/07/dns_poisoning_scam_raises_wariness_of_pharming.html).
68. Andy Sullivan, « Con artists dial for dollars on Net Phones », *Reuters*, 20 mars 2005. <http://msnbc.msn.com/id/7235764/>.
69. Brightmail, « Brightmail to Provide Data to EarthLink to Power Anti-Phishing Toolbar », communiqué de presse, 19 avril, 2004.
70. Voir par exemple APACS, « New Trojan Email Attack targets On-line Baking Customers », communiqué de presse, 13 août 2004. <http://www.apacs.org.uk/>. Un exemple d'attaque par hameçonnage peut être observé à l'adresse : [http://news.netcraft.com/archives/2005/03/07/phishers\\_use\\_wildcard\\_dns\\_to\\_build\\_convincing\\_bait\\_urls.html](http://news.netcraft.com/archives/2005/03/07/phishers_use_wildcard_dns_to_build_convincing_bait_urls.html).
71. <http://www.antiphishing.org>.

72. APWG, Commentary to FDIC « Putting an End to Account-Hijacking Identity Theft », 4 février 2005.
73. <http://www.trustwatch.com/>.
74. [http://pages.ebay.com/ebay\\_toolbar/](http://pages.ebay.com/ebay_toolbar/).
75. Dennis Fisher, « IE 7: No Phishing Allowed », 21 février 2005, <http://www.eweek.com/article2/0,1759,1766250,00.asp>.
76. <http://www.aa419.org/fake-banks/fakebankslist.php?start=1>.
77. APACS, « UK card fraud losses reach £504.8m », 8 mars 2005 [http://www.apacs.org.uk/about\\_apacs/htm\\_files/pressreleases.htm](http://www.apacs.org.uk/about_apacs/htm_files/pressreleases.htm).
78. « U.S. Consumer Loss of phishing Fraud to Reach \$500 Million », 29 septembre 2004, [http://www.truste.org/about/press\\_release/09\\_29\\_04.php](http://www.truste.org/about/press_release/09_29_04.php).
79. Gartner, « Gartner Study Finds Significant Increase in E-Mail Phishing Attacks », 6 mai 2004. [http://www3.gartner.com/5\\_about/press\\_releases/asset\\_71087\\_11.jsp](http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp).
80. TowerGroup, « Fraud Losses from email phishing attacks to total USD 137 million globally in 2004, Lower than other estimates », 1er décembre 2004. [http://www.towergroup.com/public/presscenter/default\\_press.asp](http://www.towergroup.com/public/presscenter/default_press.asp).
81. Out-Law.com, octobre 2004, signalant la publication des statistiques de l'APACS : [http://www.out-law.com/php/page.php?page\\_id=apacslaunchesanti1096883491&area=news](http://www.out-law.com/php/page.php?page_id=apacslaunchesanti1096883491&area=news).
82. Gartner, Op.cit. [http://www3.gartner.com/5\\_about/press\\_releases/asset\\_71087\\_11.jsp](http://www3.gartner.com/5_about/press_releases/asset_71087_11.jsp).
83. « U.S. Consumer Loss of phishing Fraud to Reach \$500 Million », Op.cit.
84. Duane Wessels, « Searching for DNS Cache Poisoners », DNS-OARC Workshop, Santa Clara, 25-26 juillet 2005. <http://www.caida.org/projects/oarc/200507/slides/oarc0507-Wessels-poisoning.pdf>
85. Ibid et <http://www.measurement-factory.com/> et <https://oarc.isc.org/>
86. Voir <http://www.ftc.gov/opa/2004/04/spywaretest.htm>.
87. FTC, « Spyware Workshop: Monitoring Software on your PC: Spyware, Adware, and Other Software », Staff Report mars 2005. <http://www.ftc.gov/os/2005/03/050307spywarerpt.pdf>.
88. <http://www.antispwarecoalition.org/>
89. <http://www.antispwarecoalition.org/definitions.pdf>
90. PTS, « Spyware and closely related phenomena », 8 avril 2005. [http://www.pts.se/Archive/Documents/EN/Spyware\\_eng.pdf](http://www.pts.se/Archive/Documents/EN/Spyware_eng.pdf)
91. John Leyden, « Spyware 'calling home' volumes soar », *The Register*, 25 juillet 2005. [http://www.theregister.co.uk/2005/07/25/spyware\\_screening/](http://www.theregister.co.uk/2005/07/25/spyware_screening/)

92. Une question que l'on peut se poser est de savoir dans quelle mesure le logiciel espion se différencie des cookies, lesquels peuvent avoir des aspects positifs pour les utilisateurs (par exemple pour enregistrer leurs préférences) mais aussi servent à enregistrer certains aspects de leur utilisation d'Internet. Parmi les différences majeures, on peut citer le fait que les cookies ne fonctionnent pas de façon malicieuse, qu'ils sont identifiables, qu'ils peuvent être supprimés à tout moment et qu'ils ne peuvent diffuser des virus ou accéder au disque dur de l'utilisateur. On aurait signalé toutefois que certains logiciels espions tentent de modifier les cookies dans le but d'en extraire des informations pour ouvrir de nouveaux comptes ou avoir accès aux comptes existants de l'utilisateur. Voir <http://www.webopedia.com/DidYouKnow/Internet/2002/Cookies.asp> et [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci861584,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci861584,00.html) et <http://www.w3.org/Security/Faq/wwwsf2.html#CLT-Q10>.
93. Voir <http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf>, page 12, consulté le 5 octobre 2004.
94. Voir <http://spywarewarrior.com/asw-test-guide.htm> (octobre 2004).
95. <http://research.pestpatrol.com/WhitePapers/Glossary.asp>.
96. <http://research.pestpatrol.com/>.
97. Bryson Gordon, McAfee Security <http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf> et <http://www.ftc.gov/bcp/workshops/spyware/gordon.pdf>.
98. Declan McCullagh, « Few solutions pop up at FTC adware workshop », 19 avril 2004, [http://news.com.com/Few+solutions+pop+up+at+FTC+adware+workshop/2100-1028\\_3-5195222.html](http://news.com.com/Few+solutions+pop+up+at+FTC+adware+workshop/2100-1028_3-5195222.html).
99. <http://www.earthlink.net/spyaudit/press/>.
100. Symantec, « Internet Security Threat Report Highlights Rise In Threats To Confidential Information », communication à la presse, 21 mars 2005, <http://www.symantec.com/press/2005/n050321.html>.
101. Matthew Fordahl, « Microsoft to make antispyware software free », Associated Press, 15 février 2005.
102. Andrew Birmingham, « The spy in your machine », 7 septembre 2004. <http://australianit.news.com.au/articles/0,7204,10665570%5E15382%5E%5Enbv%5E,00.html>. Voir également le rapport FDIC, Op.cit.
103. Dell, « Dell Launches Campaign to Build Awareness of PC Security Issues », communiqué de presse, Round Rock, Texas, 20 juillet 2004 [http://www1.us.dell.com/content/topics/global.aspx/corp/pressoffice/en/2004/2004\\_07\\_20\\_rr\\_000?c=us&l=en&s=gen&cs=#tn1](http://www1.us.dell.com/content/topics/global.aspx/corp/pressoffice/en/2004/2004_07_20_rr_000?c=us&l=en&s=gen&cs=#tn1).
104. FTC, Staff report of Spyware Workshop, Op.cit.
105. Matt Hines, « Microsoft launches anti-spyware beta », CNET, 6 janvier 2005. [http://news.com.com/Microsoft+launches+anti-spyware+beta/2100-1029\\_3-5514899.html](http://news.com.com/Microsoft+launches+anti-spyware+beta/2100-1029_3-5514899.html).
106. BBC, « UK police foil massive bank theft », 17 mars 2005. [http://news.bbc.co.uk/2/hi/uk\\_news/4356661.stm](http://news.bbc.co.uk/2/hi/uk_news/4356661.stm).
107. ISC, Handlers Diary, 27 février 2005. <http://isc.sans.org/index.php?off=worldmap>.
108. Gregg Keizer, « CoolWebSearch tops spyware threat list », Techweb, 31 mars 2005. <http://www.itnews.com.au/newsstory.aspx?CIaNCID=35&CIaNID=18386>.

109. Marco Cremonini et Patrizia Martini, « Evaluating Information Security Investments from the Attacker's Perspective », présenté au quatrième atelier sur l'économie de la sécurité de l'information, Kennedy School of Government, Harvard University, 2-3 juin 2005. <http://infoecon.net/workshop/pdf/23.pdf> et à la même conférence : Paul Judge, Dmitri Alperovitch et Weilai Yang, « Understanding and Reversing the Profit Model of Spam », <http://infoecon.net/workshop/pdf/49.pdf>.
110. La carte peut être consultée à l'adresse : <http://us.mcafee.com/virusInfo/default.asp?cid=10371>.
111. <http://securityresponse.symantec.com/avcenter/vinfodb.html>.
112. John Leyden, « Internet neighbourhood watch set up », 7 décembre 2000. [http://www.theregister.co.uk/2000/12/07/internet\\_neighbourhood\\_watch\\_set\\_up/](http://www.theregister.co.uk/2000/12/07/internet_neighbourhood_watch_set_up/).
113. <http://www.dshield.org/>.
114. <http://isc.sans.org/>.
115. <http://isc.sans.org/survivalhistory.php>.
116. [http://www.nist.gov/public\\_affairs/general2.htm](http://www.nist.gov/public_affairs/general2.htm).
117. <http://icat.nist.gov/icat.cfm?function=statistics>.
118. <https://cassandra.cerias.purdue.edu/main/index.html>.
119. <http://www.us-cert.gov/aboutus.html>.
120. <http://www.auscert.org.au/render.html?it=4125>, <http://www.cancert.ca/Home/Default.php>, <http://www.certcc.or.kr/>, <http://www.cert-ist.com>, <http://www.jpCERT.or.jp/english/>, <http://www.apCERT.org/> et <http://www.first.org/about/organization/teams/>.
121. <http://www.us-cert.gov/federal/statistics/>.
122. <http://www.jpCERT.or.jp/isdas/readme-en.html#graph>.
123. Voir par exemple : <http://www.itu.int/osg/spu/ni/security/workshop/presentations/cni.14.pdf>.
124. « IBM report: Surge in viruses and worms targeting mobile devices, satellite communications anticipated in 2005 », 9 février 2005, <http://www-1.ibm.com/services/us/index.wss/rs/imc/a1008866>.
125. <http://www.f-secure.com/v-descs/cabir.shtml>.
126. <http://www.f-secure.com/weblog/>.
127. John Markoff et Laura M Holsen, « At the Oscars, stars' phones were open book », *The New York Times* (réimpression dans l'*International Herald Tribune* du 3 mars 2005).
128. <http://www.f-secure.com/v-descs/commwarrior.shtml>.
129. <http://www.caida.org>
130. Bradley Huffaker, « Overview of CAIDA Data Collection, Analysis and Visualization », 9 juin 2005. <http://www.caida.org/outreach/presentations/2005/ijj/>

131. Michael Delio, « Find the Cost of (Virus) Freedom », *Wired*, 14 janvier 2002.  
<http://www.wired.com/news/infostructure/0,1377,49681,00.html>.
132. Le SANS Institute, « The Top 20 Internet Security Vulnerabilities and How to Eliminate Them », 2003,  
<http://www.sans.org/top20/cdipresentation.pdf>.
133. Reuters, « Virus damage estimated at \$55 billion in 2003 », 16 janvier 2004,  
<http://msnbc.msn.com/id/3979687/>.
134. Prevx, « Prevx names top ten Internet attacks of the year », 28 décembre 2004.  
<http://www.prevx.com/newspress.asp>.
135. The HoneyNet Project & Research Alliance, « Know your Enemy: Tracking Botnets », 13 mars 2005  
<http://project.honeynet.org/papers/bots/>.
136. Micah Hoffman, « BOTS – The creation of a Botnet Tracking Web Application », DNS-OARC Workshop, Santa Clara, 25-26 juillet 2005. <http://public.oarci.net/oarc/workshop-2005/minutes/hoffman-BOTS>
137. <http://www.ciphertrust.com/resources/statistics/zombie.php>.
138. Symantec, « Symantec Internet Security Threat Report Identifies More Attacks Now Targeting e-Commerce, Web Applications », 20 septembre 2004.  
<http://www.symantec.com/press/2004/n040920b.html>.
139. « IRC Botnet Found and Shutdown », 10 septembre 2004. <http://isc.sans.org/diary.php?date=2004-09-07>.
140. « Botnets: hidden menace makes PCs an instrument of extortion », 16 décembre 2004.  
[http://www.nzherald.co.nz/index.cfm?c\\_id=688&ObjectID=9003405](http://www.nzherald.co.nz/index.cfm?c_id=688&ObjectID=9003405).
141. Symantec, « Internet Security Threat Report », Trends for juillet 04 – décembre 04, Volume VII, mars 2005.
142. Netcraft, « E-commerce Firm 2Checkout Reports DDoS Extortion Attack », 17 avril 2004,  
[http://news.netcraft.com/archives/2004/04/17/ecommerce\\_firm\\_2checkout\\_reports\\_ddos\\_extortion\\_attack.html](http://news.netcraft.com/archives/2004/04/17/ecommerce_firm_2checkout_reports_ddos_extortion_attack.html).
143. « Hackers Almost Break Bookmaker », *Kommersant Daily*, 4 avril, 2005  
<http://www.kommersant.com/page.asp?id=560203> and Bill Goodwin, « Crime gangs unite to launch online attacks », 5 avril 2005.  
<http://www.computerweekly.com/articles/article.asp?liArticleID=137723&liArticleTypeID=1&liCategoryID=6&liChannelID=13&liFlavourID=1&sSearch=&nPage=1>.
144. Avi Goldfarb, « Why do denial of service attacks reduce future visits?: Switching costs versus changing preferences », communication datée de février 2005 au quatrième atelier sur l'économie de la sécurité de l'information, Kennedy School of Government, Harvard University, 2-3 juin 2005  
<http://infoecon.net/workshop/pdf/6.pdf>.
145. Netcraft, « Akamai Attack Highlights Threat From Bot Networks », 16 juin 2004,  
[http://news.netcraft.com/archives/2004/06/16/akamai\\_attack\\_highlights\\_threat\\_from\\_bot\\_networks.html](http://news.netcraft.com/archives/2004/06/16/akamai_attack_highlights_threat_from_bot_networks.html)  
and « DDoS Attack on DoubleClick Slows Many Sites », 28 juillet 2004,  
[http://news.netcraft.com/archives/2004/07/28/ddos\\_attack\\_on\\_doubleclick\\_slows\\_many\\_sites.html](http://news.netcraft.com/archives/2004/07/28/ddos_attack_on_doubleclick_slows_many_sites.html).

146. <http://www.fbi.gov/mostwanted/fugitive/jan2005/janechouafni.htm> and Netcraft, « Botnet with 10,000 Machines Shut Down », 8 septembre 2004.  
[http://news.netcraft.com/archives/2004/09/08/botnet\\_with\\_10000\\_machines\\_shut\\_down.html](http://news.netcraft.com/archives/2004/09/08/botnet_with_10000_machines_shut_down.html).
147. Elizabeth Biddlecombe, « Criminal use of spam increasing – experts », Total Telecom, 31 janvier 2005,  
<http://www.totaltele.com/view.asp?ArticleID=115625&pub=tt&categoryid=0>.
148. John Leyden, « Botnets strangle Google Adwords », *The Register*, 3 février 2005.  
[http://www.theregister.co.uk/2005/02/03/google\\_adwords\\_attack/](http://www.theregister.co.uk/2005/02/03/google_adwords_attack/).
149. Dan Ilet, « Organised crime’s grip on the Net ‘is tightening’ », 9 décembre 2004,  
<http://news.zdnet.co.uk/0,39020330,39180206,00.htm> and Netcraft « Fraud Hosting Services widely promoted », 1er mars 2004,  
[http://news.netcraft.com/archives/2004/03/01/fraud\\_hosting\\_services\\_widely\\_promoted.html](http://news.netcraft.com/archives/2004/03/01/fraud_hosting_services_widely_promoted.html).
150. Ilet, « Organised crime's grip on the Net ‘is tightening’ », Op.cit.
151. Elizabeth Biddlecombe, « Criminal use of spam increasing – experts », Op.cit; Reuters, « Scotland Yard and the case of the rent-a-zombies », 7 juillet 2004, [http://news.zdnet.com/2100-1009\\_22-5260154.html](http://news.zdnet.com/2100-1009_22-5260154.html);  
James Robertson, « Zombies join the attack », 8 janvier 2005,  
<http://www.smh.com.au/news/Icon/Zombies-join-the-attack/2005/01/04/1104601351920.html>.
152. Bill Goodwin, « Crime gangs unite to launch online attacks », 5 avril 2005.  
<http://www.computerweekly.com/articles/article.asp?liArticleID=137723&liArticleTypeID=1&liCategoryID=6&liChannelID=13&liFlavourID=1&sSearch=&nPage=1>.
153. Netcraft, « Euro 2004 Gambling Sites Hit By Denial Of Service Attacks », 10 juin 2004.  
[http://news.netcraft.com/archives/2004/06/10/euro\\_2004\\_gambling\\_sites\\_hit\\_by\\_denial\\_of\\_service\\_attacks.html](http://news.netcraft.com/archives/2004/06/10/euro_2004_gambling_sites_hit_by_denial_of_service_attacks.html) and « Botnets: hidden menace makes PCs an instrument of extortion », 16 décembre 2004.  
[http://www.nzherald.co.nz/index.cfm?c\\_id=688&ObjectID=9003405](http://www.nzherald.co.nz/index.cfm?c_id=688&ObjectID=9003405).
154. Telus, « Modem Hijacking », [http://about.telus.com/publicpolicy/scams\\_modemhijacking.html](http://about.telus.com/publicpolicy/scams_modemhijacking.html).
155. McAfee, « Virus Watch », eSecurity news, été 2004.  
<http://dispatch.mcafee.com/us/esecuritynews/summer2004/viruswatch.asp?cid=10984>.
156. McAfee, « Virus Watch », eSecurity news, été 2004.  
<http://dispatch.mcafee.com/us/esecuritynews/summer2004/viruswatch.asp?cid=10984>. Refer also to McAfee testimony at <http://www.ftc.gov/bcp/workshops/spyware/transcript.pdf>, p 74.
157. Robin Langford, « BT blocks 1000 rogue diallers », 5 octobre 2004.  
[http://www.netimperative.com/2004/10/5/BT\\_blocks\\_diallers](http://www.netimperative.com/2004/10/5/BT_blocks_diallers).
158. The eFinland Weblog, « The Consumer Should Not Have to Pay for Modem Hijacking – That an Internet-Based Test Is Charged for Has Come as a Surprise to Many », 2 août 2004.  
<http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=26518>.
159. <http://isc.sans.org/diary.php?date=2005-02-19>.
160. <http://www.phonebusters.com/english/statistics.html>.
161. <http://www.content.overture.com/d/USm/ac/index.jhtml>.
162. [http://isp.webopedia.com/TERM/C/click\\_fraud.html](http://isp.webopedia.com/TERM/C/click_fraud.html).

163. Zoltan Gyongyi et Hector Garcia-Molina, « Link Spam Alliances », Stanford University, 2 mars 2005. <http://blog.searchenginewatch.com/blog/pdf/linkalliance.pdf>
164. Rob McGann , « Impression Spam Worries Google Advertisers », *ClickZ News*, 24 février 2005. <http://www.clickz.com/news/article.php/3485386>.
165. Par exemple, Associated Press, « Click Fraud Threat Looms », 15 février 2005 <http://edition.cnn.com/2005/TECH/internet/02/15/click.fraud.ap/> et Brad Stone, « When Mice Attack », Newsweek, 24 janvier 2005 <http://msnbc.msn.com/id/6830802/site/newsweek/>.
166. Brad Stone, Op.cit.
167. Pour une analyse, voir : [http://news.netcraft.com/archives/2005/02/02/google\\_domain\\_strategy\\_could\\_impact\\_domain\\_resale\\_values.html](http://news.netcraft.com/archives/2005/02/02/google_domain_strategy_could_impact_domain_resale_values.html) et [http://news.netcraft.com/archives/2005/02/22/searchoptimized\\_domain\\_portfolio\\_sells\\_for\\_164\\_million.html](http://news.netcraft.com/archives/2005/02/22/searchoptimized_domain_portfolio_sells_for_164_million.html).
168. « Report Details New Threats to Data Security », 8 mars 2005, [http://www.govtech.net/magazine/channel\\_story.php?channel=4&id=93314](http://www.govtech.net/magazine/channel_story.php?channel=4&id=93314).
169. <http://www.iab.net/standards/measurement.asp>.
170. Brad Stone, Op.cit.
171. SEMPO, « The State of Search Engine Marketing – 2004 », janvier 2005. <http://www.sempo.org/research/sem-trends-2004.php> et « Click Fraud, an Industry Crisis, or Blip on the Search Engine Marketing Landscape? », 23 février 2005. <http://www.sempo.org/press/click-fraud.php>.
172. <http://www.pewinternet.org/PPF/p/1052/pipcomments.asp>.
173. Les résultats proviennent d'une enquête de suivi mensuel par le *Pew Internet & American Life Project*. Au total, 2 201 adultes âgés de 18 ans et plus ont participé à l'enquête par téléphone.
174. <http://www.mobilespam.org/>.
175. Netscape donne une présentation de SSL à l'adresse : <http://developer.netscape.com/docs/manuals/security/sslin/contents.htm> et <http://wp.netscape.com/security/techbriefs/ssl.html>.
176. <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>.
177. <http://www.fr.lastminute.com/lmn/pso/catalog/Category.jhtml?CATID=98185>.
178. <http://www.lastminute.com/lmn/banner/security/securityg.htm>.
179. David Johnson, « A Modest Approach to SSL Certificate Costs », [http://www.workz.com/cgi-bin/gt/pl\\_page.html.template=1&content=2133&nav1=1&](http://www.workz.com/cgi-bin/gt/pl_page.html.template=1&content=2133&nav1=1&).
180. Netcraft, « Do SSL Certificate Authorities still have a margin generating business model? », 9 septembre 2003, [http://news.netcraft.com/archives/2003/09/09/do\\_ssl\\_certificate\\_authorities\\_still\\_have\\_a\\_margin\\_generating\\_business\\_model.html](http://news.netcraft.com/archives/2003/09/09/do_ssl_certificate_authorities_still_have_a_margin_generating_business_model.html).

181. « Go Daddy Launches Low-Priced, 128-Bit Turbo SSL Certificates With Issuance in Minutes », communiqué de presse, 15 septembre 2004 [http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/09-15-2004/0002250580&EDATE=.](http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/09-15-2004/0002250580&EDATE=)
182. <http://www.ev1servers.net/english/starterssldetails.asp>.
183. Netcraft, Secure Server Report, avril 2005.
184. Ibid.
185. ACCESS Co., Ltd, « ACCESS NetFront Browser Powers First 3G Smart-Card Handset From NTT DoCoMo », communiqué de presse, 1er septemnre 2004. <http://www.symbianone.com/index.php?option=content&task=view&id=748>.
186. GeoTrust, « GeoTrust Announces Power Server ID™ SSL Certificate with Expanded Support for Mobile Computing », communiqué de presse, 20 juillet 2004, [http://www.geotrust.com/news\\_events/press/pr\\_power\\_server\\_id\\_071904.htm](http://www.geotrust.com/news_events/press/pr_power_server_id_071904.htm).
187. <http://www.secgo.com/ebanking/english/>.
188. [http://epp.eurostat.cec.eu.int/portal/page?\\_pageid=1996,45323734&\\_dad=portal&\\_schema=PORTAL&screen=welcomeref&open=/&product=EU\\_MAIN\\_TREE&depth=1](http://epp.eurostat.cec.eu.int/portal/page?_pageid=1996,45323734&_dad=portal&_schema=PORTAL&screen=welcomeref&open=/&product=EU_MAIN_TREE&depth=1).
189. <http://www.abs.gov.au/Ausstats/abs@.nsf/Lookup/D4F295CE33FAC665CA256E59007AC471> et <http://www.abs.gov.au/Ausstats/abs@.nsf/Lookup/45C825409149033FCA256889000B8132>.
190. [http://www.johotsusintokey.soumu.go.jp/tsusin\\_riyou/data/eng\\_tsusin\\_riyou02\\_2003.pdf](http://www.johotsusintokey.soumu.go.jp/tsusin_riyou/data/eng_tsusin_riyou02_2003.pdf).
191. [http://www.johotsusintokey.soumu.go.jp/tsusin\\_riyou/data/eng\\_tsusin\\_riyou01\\_2003.pdf](http://www.johotsusintokey.soumu.go.jp/tsusin_riyou/data/eng_tsusin_riyou01_2003.pdf).
192. <http://www.ntia.doc.gov/ntiahome/dn/html/anationonline2.htm>.