Les pirates du cyberespace

par Frédérick DOUZET, Jean-Loup SAMAAN et Alix DESFORGES

| Éditions La Découverte | *Hérodote*

2009/3 - n° 134
ISSN 0338-487X | ISBN 9782707158444 | pages 176 à 193

Pour citer cet article :
— Douzet F., Samaan J.-L. et Desforges A., Les pirates du cyberespace, *Hérodote* 2009/3, n° 134, p. 176-193.

Distribution électronique Cairn pour Éditions La Découverte.

Les pirates du cyberespace

Frédérick Douzet, Jean-Loup Samaan**
et Alix Desforges****

Fini le temps des *hackers* romantiques et libertaires, Robin des Bois modernes de la communication. Le nouveau visage de la piraterie dans le cyberespace, pour les médias occidentaux, c'est la Chine ! En mars 2009, des chercheurs de l'université de Toronto (Canada) annoncèrent avoir démantelé un réseau de cyberespionnage, baptisé GhostNet, contrôlé à partir de quatre serveurs dont trois basés en Chine. Le réseau aurait infiltré près de 1 300 ordinateurs dans 103 pays, dont celui du dalaï-lama. Les pirates auraient infecté les ordinateurs à l'aide d'un cheval de Troie, un logiciel malveillant – *malware* – qui, installé clandestinement sur un ordinateur, permet de recueillir des informations confidentielles en toute discrétion, voire de prendre contrôle de la machine pour lancer des attaques vers d'autres serveurs [Information Warfare Monitor, 2009].

Dans un contexte de dépendance accrue aux outils informatiques et d'interconnexion des systèmes au niveau mondial, la cyberpiraterie est devenue un enjeu sécuritaire majeur pour les États. La course à la maîtrise de l'information s'inscrit dans un contexte de rivalités de pouvoir entre des États-nations qui s'efforcent d'assurer leur défense, de faire respecter leurs lois et de servir leurs intérêts économiques et politiques. Dans ce domaine comme dans d'autres, la Chine, championne de la censure du Net, cherche à affirmer sa puissance, suscitant les fantasmes les plus extravagants et les plus sérieuses inquiétudes.

---

* Maître de conférences à l'Institut français de géopolitique, université Paris-VIII. Membre junior de l'Institut universitaire de France.

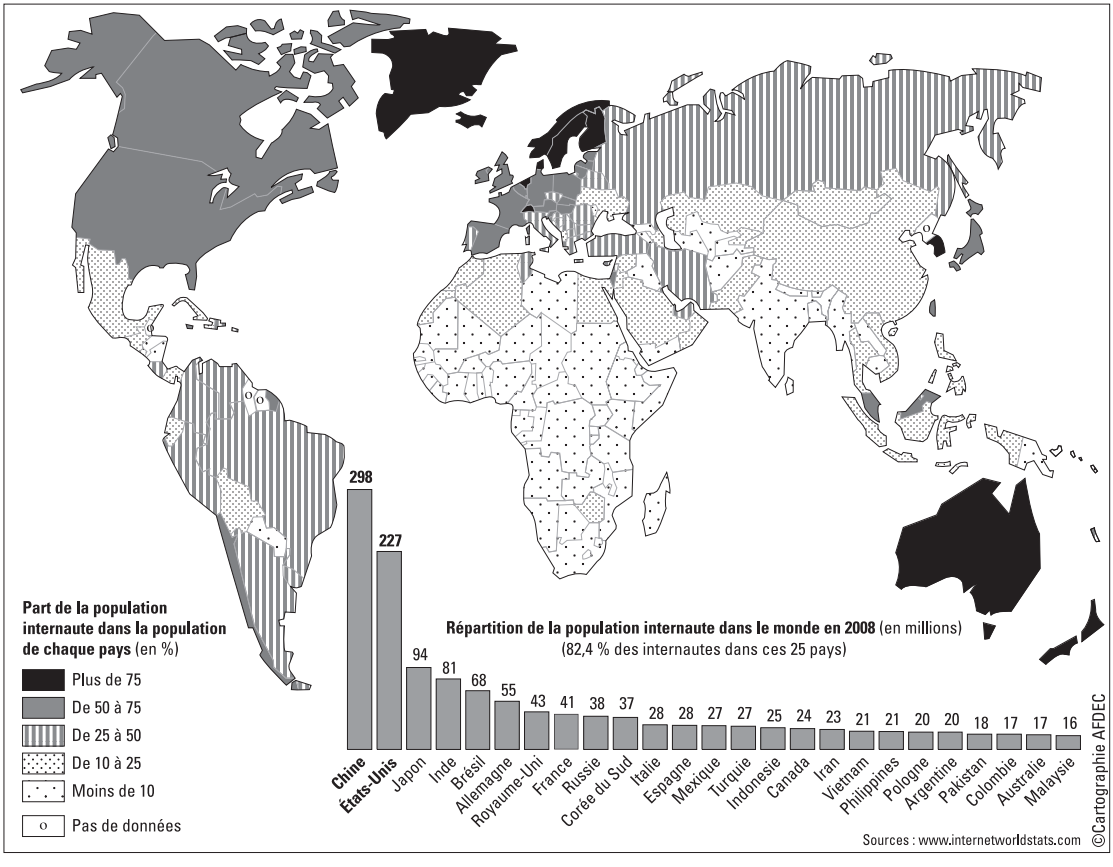
** Docteur en science politique. Chercheur à l'université Paris-I, il a été *visiting scholar* à Duke University (2006) et à la RAND Corporation (2007-2008). Il a publié *Les Métamorphoses du Hezbollah* (Karthala).

*** Chercheuse à l'Institut français de géopolitique, université Paris-VIII.

Hérodote, n° 134, La Découverte, 3e trimestre 2009.

Hérodote, n° 134, La Découverte, 3e trimestre 2009.

Carte 1. – Pénétration de l'Internet en 2008 et poids de la population internaute dans le monde en 2008



« Le cyberespace est une véritable vulnérabilité de l'économie et du gouvernement américains, dans la mesure où tous deux dépendent fortement de l'utilisation des ordinateurs et de leur connexion à l'Internet », note le rapport au Congrès de la commission sur l'économie et la sécurité US-Chine [USCC 2008, p. 9]. Or la Chine développerait activement un programme de cyberespionnage et ses progrès seraient tels qu'elle pourrait « mener des formes de cyberguerre tellement sophistiquées que les États-Unis pourraient se révéler incapables de les contrer ni même de les repérer » (*ibid.*, p. 164). La supériorité chinoise pourrait « amoindrir la prépondérance militaire actuelle des États-Unis » (*ibid.*, p. 9).

Et pourtant, comme nous le verrons, la localisation des pirates est fort complexe et les pirates qui sévissent à travers le cyberespace sont loin d'être exclusivement concentrés en Chine, de même que le piratage n'est pas limité au cyberespionnage. Les attaques contre l'Estonie en avril 2007 ou contre la Géorgie en 2008 provenaient fort probablement de réseaux russes, sans que l'on sache précisément desquels. Des réseaux internationaux émanent d'autres territoires, parfois inattendus, en fonction de la nature de leurs intrusions, des ressources disponibles ou de rivalités géopolitiques spécifiques, comme nous le verrons grâce à des cartes originales. Le piratage prend des formes variées, plus ou moins sophistiquées, qui n'ont de limites que l'imagination et les compétences techniques de leurs protagonistes.

Toutes les formes de piraterie ne relèvent pas du champ de la géopolitique, certaines sont des actes criminels qui empruntent le véhicule de l'Internet sans qu'ils relèvent ou suscitent de rivalités de pouvoir sur des territoires. Il est parfois d'ailleurs complexe de déterminer à partir de quel moment un certain type de cybercriminalité devient une question géopolitique. Inversement, les enjeux géopolitiques du cyberespace ne sont pas tous liés à la piraterie. Le *cyberplanning* qui permet aux réseaux terroristes comme Al-Qaïda de s'organiser, lever des fonds, coordonner des attaques peut avoir recours à la piraterie mais pas nécessairement. Les conflits autour de la maîtrise de l'adressage des noms de domaines[1], des limites de la liberté d'expression (comme par exemple à l'égard des mouvements nazis) ou encore la surveillance et le fichage des utilisateurs ne relèvent pas de la piraterie.

Pour ce numéro « Pillage et piraterie », nous avons choisi de nous consacrer exclusivement aux enjeux de la piraterie dans le cyberespace, ce qui nécessite avant tout d'expliquer en quoi le cyberespace peut être considéré comme un

1. Les ordinateurs possèdent une adresse IP (Internet Protocol) numérique qui s'écrit également sous forme de noms de domaines explicites permettant d'identifier les machines connectées aux réseaux. Les dernières lettres (.fr, .uk, .com, .edu) correspondent généralement à un pays ou un secteur d'activités.

champ d'action des pirates. Nous montrerons ensuite quels sont leurs différents modes d'action et les enjeux géopolitiques qui y sont liés. Nous verrons enfin pourquoi il est si complexe pour les États – souvent à la fois victimes et protagonistes – de contrer les pirates, pour des raisons tout aussi géopolitiques que techniques.

Représentations de la piraterie dans le cyberespace

Piratage et piraterie vont souvent de pair à propos du cyberespace. Or les deux termes recouvrent des enjeux sensiblement différents, bien que la racine soit commune et qu'ils soient, par analogie, plus ou moins interchangeables. La piraterie désigne l'acte de brigandage maritime et, appliqué à la navigation aérienne, le détournement d'avion. Au sens figuré, il fait aussi référence à l'escroquerie *(Petit Robert)*. Le piratage désigne plus précisément le vol effronté, l'accaparement illégal et par la force du bien d'autrui, ou encore du contenu d'œuvres intellectuelles ou artistiques (source CNRTL). Les deux termes peuvent s'appliquer aux pirates du cyberespace, celui de piratage étant cependant le plus communément utilisé en français.

Comme les mers, les airs et les océans, le cyberespace, aussi virtuel soit-il, est un territoire de la navigation. Le vocabulaire est explicite : on navigue sur le Net, on surfe... Et les pirates prennent d'assaut, immobilisent, détournent et pillent ses serveurs, parfois par seule effronterie, parfois pour des raisons criminelles, parfois pour des raisons géopolitiques. Le terme cyberespace apparut pour la première fois sous la plume d'un écrivain américain, William Gibson, dans son premier roman *Neuromancer* (1984). Il désignait une représentation mentale des données et de l'information stockées au cœur des systèmes informatiques de toute l'humanité, un espace tridimensionnel « d'une infinie complexité », généré électroniquement, dans lequel ses personnages entraient en se connectant par ordinateur. Le cyberespace désigne depuis le territoire virtuel, hors du monde physique, dans lequel se déroulent les échanges et interactions entre internautes, mais aussi les affrontements, les rivalités de pouvoir ainsi que les escroqueries diverses et vols de propriété intellectuelle ou artistique assimilés au piratage.

Le cyberpirate, héros libertaire

Le pirate du cyberespace a cependant longtemps bénéficié d'une image positive, celle d'un héros romantique et libertaire, féru de technologie, qui, à lui seul, peut faire vaciller les empires les plus puissants. Le *hacker* du romancier Steven

Levy [Levy, 1984], avant même la démocratisation de l'Internet, se rebelle contre les figures d'autorité pour défendre l'accès total et illimité à l'informatique et à l'information. Le piratage est quasiment élevé au rang de forme d'art. Au début des années 1990, les pionniers du Net véhiculent des valeurs similaires : libre circulation de l'information, aucune restriction dans les échanges, extraterritorialité qui prémunit contre les lois des territoires physiques. John Perry Barlow, fondateur de l'Electronic Frontier Fondation (EFF), groupe de défense des libertés civiles dans le monde digital, alla jusqu'à publier une déclaration d'indépendance du cyberespace. Il faut souligner que le concept de contrôle va totalement à l'encontre des principes fondateurs du Net, conçu le plus solidement possible pour qu'il puisse croître. Or sa distribution en maillage, dépourvue de centre et donc de « cerveau », garantissait que l'information puisse continuer de circuler même en cas de destruction d'une de ses branches, les petits paquets d'information pouvant toujours emprunter une autre route pour arriver à destination. Les tentatives de contrôle de l'Internet par l'État américain furent activement contrées par l'EFF au nom de la démocratie et de la liberté prônées par la Constitution des États-Unis. Le débat sur la cryptographie fait rage, opposant les impératifs de sécurité des États à la protection de la vie privée.

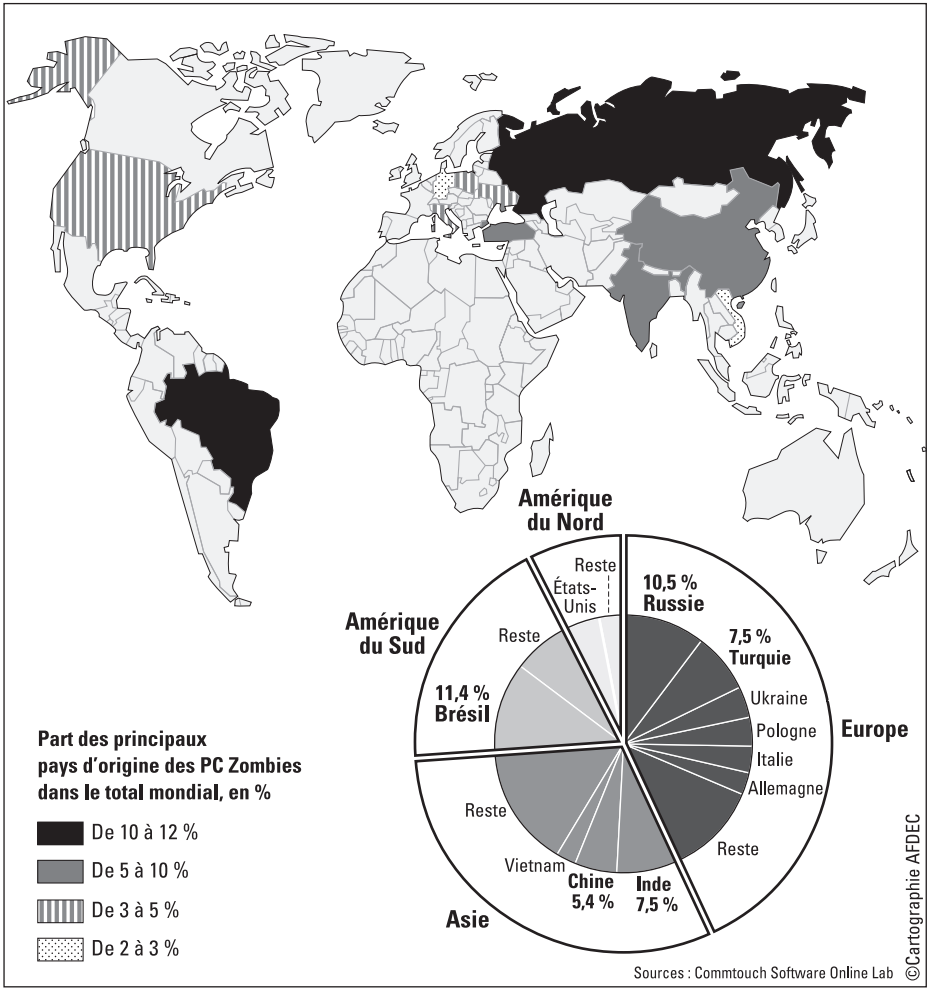
À partir de 1996, le Web commence à se développer et l'Internet à croître de façon exponentielle à travers le monde, sans que le grand public n'en saisisse encore les enjeux. La plupart des séries policières introduisent un champion des systèmes informatiques parmi leurs personnages, capable de cracker n'importe quel système pour obtenir des informations confidentielles. Les romans (l'anthologie de nouvelles *Hackers, Net Force* de Tom Clancy, *Digital Fortress* de Dan Brown, *Snow Crash* de Neal Stephenson...), les films *(War Games, The Net, The Matrix, Hackers, Anti-Trust, Die Hard 4, Firewall...)*[2] glorifient la figure du *hacker* qui défie les systèmes informatiques et l'autorité ou alimentent les fantasmes sur les risques pour les libertés civiles, la sécurité, voire la civilisation. Ils donnent même naissance à un nouveau genre littéraire, *cyberpunk*, contraction de *cybernetics* et *punk*, titre d'un roman de Bruce Bethke en 1983.

2. Pour une sélection des meilleurs et pires films sur l'Internet, voir : http ://www.pcworld.com/article/153368/the_best_and_worst_movies_about_the_internet.html.

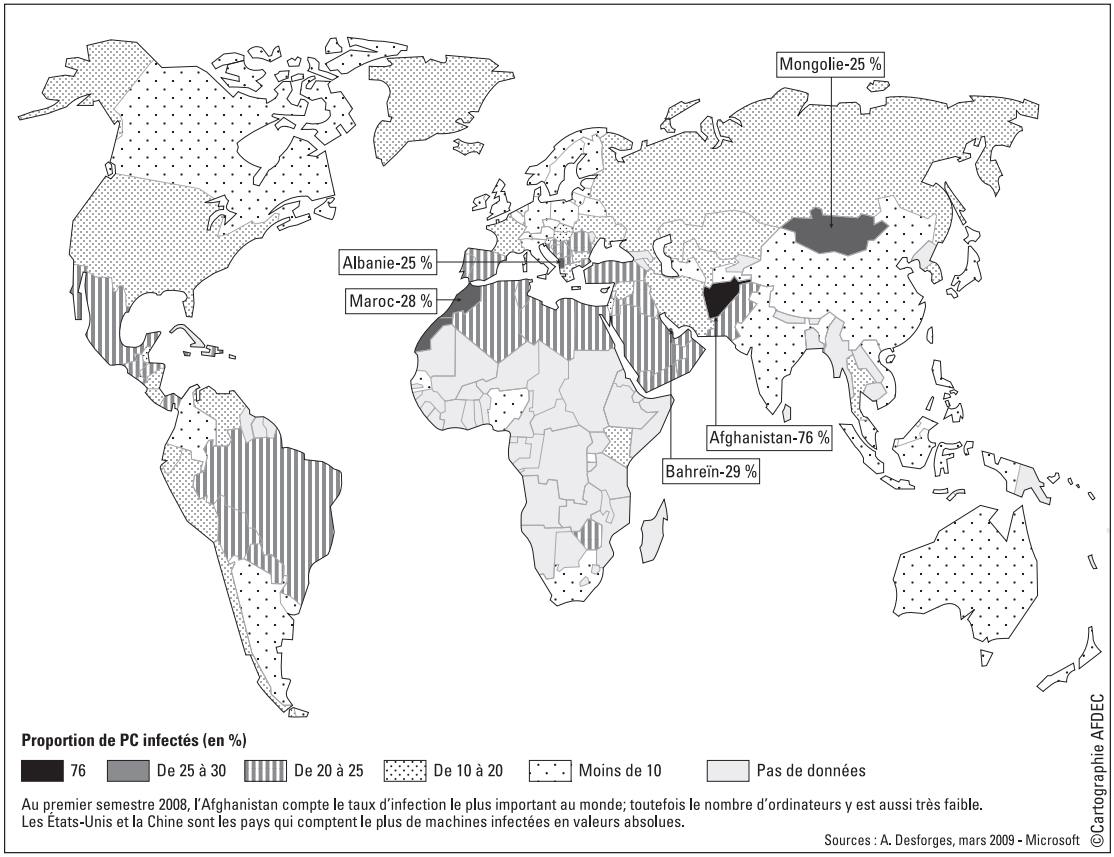
Hérodote, n° 134, La Découverte, 3e trimestre 2009.

Comment les pirates envahissent nos ordinateurs

CARTE 2. – RÉPARTITION DES PC ZOMBIES PAR PAYS D'ORIGINE DE L'ADRESSE IP EN 2008



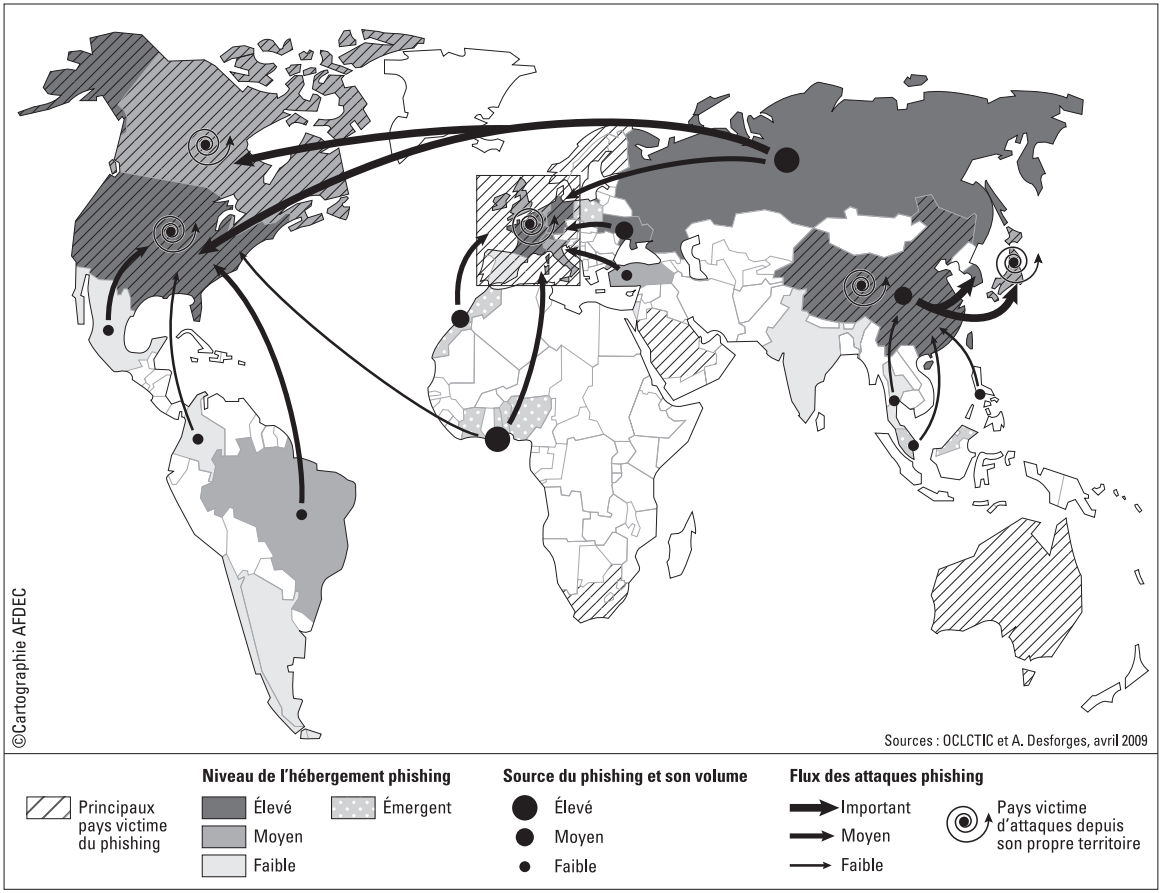
Carte 3. – Taux d'infection des ordinateurs par pays au premier semestre 2008



L'arrivée d'une connexion Internet dans la plupart des foyers rend aujourd'hui la question de l'intrusion et de la piraterie beaucoup plus tangible pour les citoyens, maillons faibles du système pour les experts car trop peu méfiants. Tous ont pourtant un jour été confrontés – parfois à leur insu – aux pratiques des pirates, sans nécessairement en être victimes. Les logiciels malveillants (*malware*) sont conçus dans le but de nuire à un système informatique et sont l'outil principal des pirates. Vers, virus ou chevaux de Troie, ils peuvent servir à détruire le fonctionnement d'un ordinateur, en prendre le contrôle pour espionner, pirater ou modifier des informations ou pour attaquer d'autres machines, généralement à l'insu de son propriétaire. Cette dernière fonction peut servir à créer un réseau d'ordinateurs infectés (*botnet* ou *PCZombies*) qui attaquent simultanément un serveur afin de le saturer jusqu'à ce qu'il ne puisse plus répondre aux demandes des utilisateurs (attaque en déni de services[3]). Ces logiciels sont souvent introduits sur les ordinateurs par le biais de spam, courriel envoyé automatiquement au plus grand nombre possible. Ces spams qui remplissent les boîtes aux lettres – ils constituent 85 % des échanges électroniques [Security Labs] – sont souvent jugés inoffensifs par les utilisateurs. Il suffit pourtant de cliquer sur un lien ou d'ouvrir une pièce jointe pour que l'ordinateur soit infecté s'il s'agit d'un spam viral. Il en existe également deux variantes : les *scams*, qui sont des spams visant à escroquer l'argent des victimes (fausses loteries, arnaques, faux investissements, faux médicaments...) ; et le *phishing*, qui consiste à envoyer un message en se faisant passer pour une banque afin de recueillir les informations bancaires à partir d'un lien contenu dans le message, pour les utiliser ensuite de façon frauduleuse. Ces procédés s'ajoutent à la reproduction et la diffusion illégales d'œuvres (musique, films, jeux vidéo...) piratées sur l'Internet, qui a valu à la Chine une plainte des Américains devant l'Organisation mondiale du commerce. Certaines de ces pratiques sont de la criminalité sans véritable dimension géopolitique. D'autres, en revanche, sont le fruit ou l'instrument de rivalités de pouvoir et relèvent des stratégies de sécurité des États.

3. Lorsque plusieurs machines attaquent un serveur on parle de déni de service distribué *(DDoS attack)*. L'attaque en déni de service distribué permet d'accélérer la mise hors service du serveur en multipliant les requêtes.

CARTE 4. – LE *PHISHING* DANS LE MONDE



La cyberpiraterie, un problème géopolitique

Si l'on s'en tient à une typologie basique des actes de cyberpiraterie, on pourrait présenter le phénomène selon leur finalité stratégique telle que : 1/ la cyberpiraterie frauduleuse (*spams, scams, phishing*) ; 2/la cyberpiraterie de renseignement (intrusions dans les systèmes d'information et communication ennemis) ; 3/la cyberpiraterie stratégique ou cyberguerre (altération ou destruction des réseaux adverses).

La cyberpiraterie frauduleuse postcoloniale

Dans le premier cas, la dimension géopolitique n'est pas nécessairement évidente. Ce type de cyberpiraterie peut en effet relever exclusivement de la fraude financière mais il peut également prendre une ampleur qui engendre des conséquences géopolitiques ou bien être motivé par des rivalités de pouvoir géopolitiques. Les arnaques sur Internet en sont le meilleur exemple. Ces infractions ont proliféré en France au cours de ces dernières années et la crise économique mondiale agit comme un véritable accélérateur du phénomène. Les arnaques apparaissent un moyen facile de gagner de l'argent rapidement pour des victimes de la crise économique amenées à trouver de nouveaux modes de financement. D'autre part, la crédulité des victimes est d'autant plus importante que l'annonce d'un gain facile, reçue par courrier électronique, suscite une moindre méfiance. Potentiellement, il y a donc à la fois plus d'arnaqueurs mais également plus de victimes.

Il existe principalement deux types d'arnaques sur Internet : celles qui sont réalisées *via* des sites d'enchères en ligne et celles qu'on appelle *« scams »*. Les *scams* sont des arnaques réalisées à partir de spam (courrier non sollicité) et font appel à la crédulité voire la cupidité des gens. Il peut s'agir de faire croire à un faux héritage, à un gain à une loterie ou encore à de faux sentiments amoureux, voire un faux deuil. Ce type d'arnaques existe depuis longtemps et les *scammers* (ceux qui pratiquent ces arnaques) ne font que s'adapter aux moyens modernes de communication ainsi qu'au contexte politique et historique. On pouvait les trouver sous le nom de « prisonnière espagnole » au XVI^e^ siècle ou encore de « lettres de Jérusalem » au XVIII^e^ et XIX^e^ siècle. Aujourd'hui, Internet offre un terrain de jeu mondial à ces pirates. Les arnaques trouvent donc une origine géographique mondiale. Dans le cas de la France, il existe deux principales sources : la Roumanie et l'Afrique de l'Ouest. Les auteurs de ces arnaques se trouvent évidemment aussi en France, l'usage de la même langue est un avantage pour commettre une arnaque mais la langue ne constitue en rien une barrière.

Pour preuve, les pirates roumains ne sont en rien dépendants de la langue de leurs victimes. Ils opèrent dans toute l'Europe grâce aux traducteurs en ligne mais aussi à leur réseau de migrants. Ils sont principalement à l'origine des arnaques *via* des sites d'enchères en ligne. En ce qui concerne l'Afrique de l'Ouest, la langue paraît jouer un rôle beaucoup plus important. Mais, plus que la langue, c'est avant tout le passé colonial de ces pays (Côte-d'Ivoire, Bénin, Togo, Ghana, Nigeria) qui est primordial.

Les pirates de ces pays pratiquent essentiellement des *scams* dans un rapport postcolonial. En effet, les *scammers* des pays colonisés par la France trouvent la majorité de leurs victimes dans les pays francophones (France, Belgique) alors que ceux des pays colonisés par la Grande-Bretagne sont tournés vers les pays anglophones (Grande-Bretagne, Irlande, États-Unis...). De plus, leurs représentations font également référence à ce rapport postcolonial. Pour eux, « les Blancs ont toujours de l'argent » et ils ont le sentiment de reprendre légitimement ce qu'on leur a pris. Il ne s'agit pas seulement d'arnaquer une victime mais d'« arnaquer le Blanc », le « colonisateur ». Ils font généralement appel aux représentations des Européens sur l'Afrique, en particulier pour les *scams* à l'héritage, également appelé « lettres nigérianes ». Ils font croire à leur victime qu'elle va toucher, entièrement ou en partie grâce à son aide, un héritage. Pour justifier cet héritage, ils prétendent à la mort ou l'emprisonnement d'un militaire, diamantaire, exportateur de canne à sucre, de coton, etc. Ils évoquent comme circonstance un conflit, un coup d'État, ou même une maladie (sida, etc.). Ils mobilisent les diverses représentations de l'Afrique, à savoir celles d'un continent fragile, politiquement instable et touché par les grandes épidémies. Malheureusement, de simples arnaques peuvent se terminer de façon dramatique (meurtre, suicide, enlèvement, emprisonnement pour les victimes).

La plupart de ces arnaqueurs opèrent depuis un cybercafé, même si on assiste à une professionnalisation de la méthode avec l'utilisation d'ordinateurs portables et de clés 3G. Néanmoins, ces pirates-là sont loin de la représentation du jeune génie informatique : la plupart du temps, leur niveau d'éducation est limité. En outre, les pays depuis lesquels ils opèrent sont également peu développés technologiquement : faible pénétration de l'Internet, lenteur des connexions, peu de formations d'ingénieur... Malgré tout, ils savent utiliser la meilleure des protections pour ne pas se faire prendre : la frontière. En opérant depuis un pays différent de celui de la victime, ils profitent non seulement du manque de moyens policiers dans leur pays mais aussi de la difficile mise en place d'une coopération policière entre deux voire trois pays. Ils utilisent également, pour la plupart, des boîtes mail du moteur de recherche Yahoo !, ce qui leur permet de stocker leurs données sur un serveur américain et non sur leur propre ordinateur. Cette manœuvre leur permet de mettre un obstacle de plus à l'enquête.

Enfin, il reste difficile de déterminer ce qu'il advient de l'argent ainsi obtenu. Il s'agit probablement principalement d'un usage personnel destiné à faire vivre sa famille et agrémenter son quotidien. De fait, cet argent est réinvesti dans l'économie locale. Mais on peut se demander si certaines sommes ne pourraient pas servir à acheter des armes, financer des organisations criminelles voire terroristes. Cependant, ces dernières pistes semblent pour l'instant rester du domaine de l'hypothèse, voire du fantasme, ou alors ne sont le fait que d'une petite minorité.

Quand la cyberpiraterie devient un acte stratégique

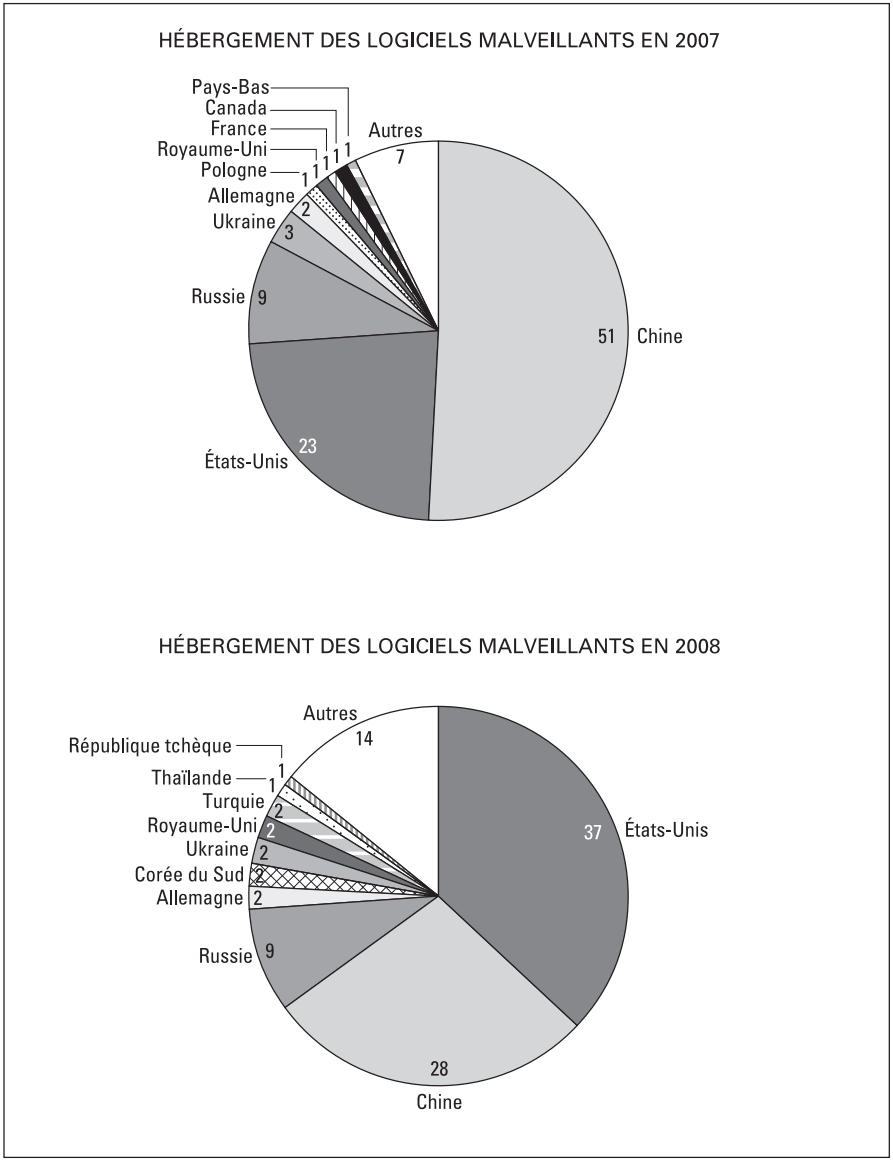
La cyberpiraterie de renseignement ou la cyberguerre ont une dimension géopolitique plus évidente. Pour autant, l'analyse politique des actes de cybercriminalité reste à ce jour un exercice difficile tant elle est menacée par la sous-interprétation de l'intentionnalité – un simple acte isolé d'individus ou de groupuscules – comme par sa surinterprétation – un acte guidé par des intérêts politiques. Force est de constater que l'on fait face à ce dilemme dans la plupart des situations contemporaines. Ainsi, la cyberattaque contre les serveurs gouvernementaux de l'Estonie en avril 2007 peut se lire selon deux angles : une attaque provenant de hackers nostalgiques de l'ère soviétique ou une opération indirecte de la Russie poutinienne afin d'intimider le Parti de la réforme estonien. Le déplacement programmé de la statue du « soldat de bronze » soviétique, héros de la Seconde Guerre mondiale, par le Parti de la réforme estonien, vainqueur des élections la même année, a autant pu aviver les foudres de dissidents isolés que celles des dirigeants à Moscou. C'est pourquoi, deux ans plus tard, l'observateur peut très bien réduire cette offensive à un acte de cyberpiraterie et non à une « troisième guerre mondiale passée inaperçue », comme Jaak Aaviksoo, ministre de la Défense estonien, s'est empressé de la qualifier[4].

Il en est de même pour le fameux rapport canadien « Tracking GhostNet », publié en mars 2009 et consacré au réseau de cyberespionnage prétendument chinois couvrant plus d'un millier d'ordinateurs, dont une centaine comprendrait ceux de diplomates européens, de représentants politiques parmi lesquels le dalaï-lama[5]. Cette enquête de dix mois a été menée par des ingénieurs en informatique bénéficiant d'un accès privilégié aux autorités tibétaines. Retraçant l'origine de ces intrusions, ces derniers ont découvert que 70 % des serveurs de contrôle derrière

4. Communiqué de presse du ministère estonien de la Défense, « Internet : XXI[st]-Century Battlefield », 16 juin 2007.

5. Information Warfare Monitor, 2009.

SCHÉMA 2. – HÉBERGEMENT DE LOGICIELS MALVEILLANTS EN 2007 ET 2008



les attaques contre les organisations tibétaines disposaient d'adresses IP chinoises. Les 30 % restants proviendraient d'adresses IP aux États-Unis, en Suède, Corée du Sud et Taïwan. Si la presse internationale s'est empressée de voir dans ce rapport la preuve concrète d'un cyberespionnage chinois de grande envergure, les chercheurs canadiens restent particulièrement modérés dans leur analyse. Comme ils l'expliquent en conclusion, « GhostNet pourrait n'être qu'une suite aléatoire d'ordinateurs infectés par un individu ou un groupe sans agenda politique, qui se trouvent être par hasard pour certains des cibles stratégiques pour la Chine »[6]. D'un point de vue technique, il s'avère même plausible que les serveurs hébergés en Chine aient été employés à distance par un autre État ou des acteurs non étatiques dans un but explicite de nuire au gouvernement chinois.

Le premier obstacle pour identifier le caractère stratégique d'une attaque est technique : les moyens de traçabilité d'offensives dans le cyberespace, *via* les attaques en déni de service orchestrées par des *botnets* (*cf. supra*), ne permettent pas aujourd'hui d'identifier l'acteur à l'origine. L'expert américain Peter Wilson, chercheur à la RAND Corporation, souligne ironiquement que contre-attaquer lors de l'attaque estonienne aurait, par exemple, signifié brouiller les ordinateurs de l'université de Californie qui avaient été piratés à distance, selon le principe du *botnet*[7].

La frontière entre criminalité individuelle et offensive politique s'avère donc ténue et c'est en ce sens que la gestion bureaucratique même de la question « cyber » pose problème : doit-elle être prise en charge par les acteurs de la sécurité (police, gendarmerie), du renseignement (services intérieurs et extérieurs) ou encore de la défense (les armées) ? Le problème fondamental de la cyberpiraterie devient donc sa définition en tant que menace. Il faut ainsi se pencher sur les statistiques, les flux d'attaques pour espérer y détecter des tendances récurrentes.

Un beau cas d'étude pour déterminer la « politisation » ou non d'actions collectives dans le cyberespace reste la mobilisation sociale en avril 2009 en Moldavie. Les événements récents dans l'ancienne république soviétique nous donnent à voir comment l'espace virtuel offre des possibilités nouvelles aux acteurs non étatiques pour défier les autorités politiques. Suite à des élections remportées par le Parti communiste moldave, une vague de mécontentement populaire s'empare du pays. Le mouvement conteste la régularité de l'élection et décide de mener une campagne de protestation contre le gouvernement. Cette insurrection est aussitôt accompagnée d'une impressionnante exploitation des outils du Web 2.0 (LiveJournal, Facebook, Twitter). L'avancée des mouvements

6. Information Warfare Monitor, 2009, p. 48.
7. Entretien, Washington, mars 2009.

sociaux est décrite minute par minute, les réactions policières sont filmées en direct, les analyses *a posteriori* et revendications subséquentes sont diffusées à travers le monde si bien que Nathan Hodge, du magazine américain *Wired*, a constaté que l'on pouvait détecter des informations relatives à la contestation moldave toutes les secondes sur Internet. Il n'en a pas fallu plus pour que l'on parle de « la révolution Twitter moldave ». Dans le cas moldave, différent de GhostNet ou de l'offensive contre l'Estonie, la subversion des technologies de l'information poursuivait un but clairement politique.

En ce sens, la cyberpiraterie comme phénomène international représente un défi pour les classiques grilles de lecture géopolitiques à deux égards : la montée en puissance des acteurs non étatiques et l'altération de la fonction des territoires.

Lutter contre la piraterie, défi technique et politique

Premièrement, les actes criminels dans le cyberespace peuvent facilement passer de la simple fraude aux agissements politiques en raison de l'extrême facilité d'accès à ces technologies. Les éléments de comparaison sont éloquents : un avion de combat coûte aujourd'hui au moins 100 millions de dollars, un système satellitaire plus d'un milliard de dollars et un navire de guerre plus de trois milliards. À l'inverse, une connexion Internet coûte moins de quarante dollars, un ordinateur performant revient à 600 dollars et n'importe quel individu avec quelques compétences en informatique peut créer un logiciel pouvant être transformé en *malware*. On peut facilement trouver sur des forums Internet des kits de cybercriminalité dont il ne reste qu'à régler quelques variables avant de le lancer. La lutte contre la prolifération informatique est tout bonnement impossible et on ne peut donc que mieux comprendre le phénomène massif de la cyberpiraterie. Celle-ci amplifie les moyens à la disposition des acteurs non étatiques (mouvements sociaux, mafias, cellules terroristes) susceptibles de troubler le fonctionnement des sociétés, voire de nuire au système international.

Enfin, à cette absence de barrière d'accès aux technologies s'ajoute la difficulté, à l'opposé, de détecter les attaques. Les ramifications internationales des *botnets* (les réseaux d'attaques en déni de service) sont telles que toute cartographie des agissements dans le cyberespace se trouve vite soumise à des limites méthodologiques. L'implication au cours d'une attaque d'une machine ou d'un réseau de machines localisé dans un pays ne signifie pas nécessairement l'implication des propriétaires de machines ou de réseaux. La mobilisation de leurs machines a pu se faire à leur insu ou bien par usurpation de l'identité de leurs machines. Il est extrêmement difficile de géolocaliser avec certitude la provenance des attaques.

Hérodote, n° 134, La Découverte, 3e trimestre 2009.

L'autre versant du problème est la difficulté politique à organiser la lutte contre la piraterie. Le premier point d'achoppement est la nécessité d'une coopération internationale entre gouvernements pour lutter contre un phénomène qui ignore les frontières terrestres, qui bâtit sa puissance et se propage hors de toute conception géographique classique de temps et d'espace. Or les États sont pris dans leur propre logique géopolitique. Les rapports de force concernant l'architecture du réseau et la gouvernance de l'Internet sont à l'origine de tensions entre les États-Unis et l'Europe à propos de la gestion des noms de domaines, sur lesquels les États-Unis gardent encore un contrôle. Les Européens réclament un plus grand partage de la gouvernance du réseau mondial avec les autres pays utilisateurs. Or la question de la gouvernance mondiale de l'Internet se heurte au fait que la majorité des pays utilisateurs ne sont pas des démocraties et qu'il est dès lors difficile d'envisager de leur donner un pouvoir sur l'architecture et la régulation du Net.

Les États cherchent aussi à affirmer leur puissance – économique, politique et militaire – et développer des capacités informationnelles susceptibles de leur offrir une supériorité stratégique dans le cadre d'un conflit, qu'il s'agisse d'activités de veille, de renseignement, de capacité d'influence politique, de déploiement stratégique ou de protection. La coopération est donc limitée par un contexte international où les rapports de force continuent de prévaloir alors même que la puissance des États est remise en question par d'autres acteurs, notamment les réseaux d'utilisateurs influents et le secteur privé. Chaque État veille à préserver sa souveraineté numérique, à savoir le contrôle sur ses réseaux et sous-réseaux (rappelons que l'Internet est un réseau de réseaux), et à assurer la sécurité et le respect de ses lois sur son territoire. Dans ce cadre, les pays développent des systèmes d'information, d'échange et d'identification des utilisateurs plus ou moins centralisés, cohérents avec leur cadre juridique et leur conception des libertés fondamentales du citoyen. Autrement dit, plus le pays est démocratique et moins l'intrusion de l'État dans les échanges privés, la centralisation des informations et le fichage des utilisateurs est toléré.

Or la lutte contre la cyberpiraterie implique une restriction de la liberté des échanges – filtres spam, pare-feu[8], blocages d'accès à certains sites – et un accroissement des capacités de surveillance et d'intrusion de la part des régulateurs. Et il n'existe pas de socle juridique commun entre les États sur lequel pourrait s'appuyer une harmonisation des pratiques. La tolérance à l'empiétement sur les libertés civiles varie d'un pays à l'autre et la mise en place de législation fait

8. Dispositif logiciel ou matériel visant à faire respecter la sécurité d'un réseau. Un pare-feu d'entreprise peut par exemple bloquer l'accès au site Facebook pour tous les employés.

l'objet d'intenses débats au sein des démocraties, comme l'a récemment montré en France l'adoption du projet de loi Hadopi perçu comme la promesse d'un filtrage de l'Internet et une menace pour la liberté d'expression. Or la protection de la liberté d'expression par le 1er amendement à la Constitution aux États-Unis, sans équivalent en France, est un puissant levier pour les groupes de défense des utilisateurs comme l'Electronic Frontier Foundation.

La question de l'identité est particulièrement sensible alors que l'interconnexion favorise la capacité à réunir des informations relevant de la sphère privée sur des citoyens et que la piraterie se base souvent sur l'usurpation d'une identité pour pénétrer un système. La cryptographie (chiffrement des messages)[9], longtemps interdite en France, révèle les tensions contradictoires du problème. Elle permet de protéger les échanges privés des pirates mais elle prive aussi d'accès les instances de sécurité lorsqu'elles sont incapables de casser les codes. Le développement des réseaux privés virtuels permet par exemple de contourner la censure dans les pays non démocratiques mais ceux-ci rendent du coup opaques les échanges entre ses utilisateurs. Démanteler un réseau de piraterie ou détecter des attaques nécessite de pouvoir remonter des filières d'échanges, pénétrer des systèmes pour identifier la source des attaques, repérer les logiciels malveillants et leurs origines. Plus la capacité de brouillage et d'anonymisation est grande, moins les pirates seront identifiables. Mais plus elle est restreinte, plus la protection des échanges privés et celle de la liberté d'échange et d'information des citoyens seront faibles.

Certaines mesures de lutte contre la piraterie peuvent enfin s'avérer contre-productives. Le projet de loi Hadopi n'est pas sans soulever quelques inquiétudes auprès d'experts qui prédisent que la loi sera au mieux inutile. Jusqu'ici, la piraterie d'œuvres musicales et cinématographiques n'engendrait pas de grands risques pour les internautes et ne nécessitait pas de grande discrétion. Mais la répression active pourrait faire naître un nouveau marché pour la création de logiciels de chiffrement, de plus en plus puissants et simples d'utilisation, qui empêcheraient la police en charge de la lutte contre la cybercriminalité de détecter la piraterie frauduleuse. Or une mise à disposition massive et gratuite de tels outils de dissimulation et d'anonymisation pourrait profiter à d'autres formes de piraterie et gêner le travail des agences en charge de la lutte contre la pédophilie, le terrorisme et autres fléaux. Les efforts techniques et financiers consentis pour développer de tels outils sont bien moindres que ceux visant à les contrer. Les conséquences budgétaires et géopolitiques pourraient être majeures.

9. La cryptographie (ou chiffrement) permet de rendre illisible un message sauf pour le destinataire qui possède la clé de décryptage.

Hérodote, n° 134, La Découverte, 3e trimestre 2009.

Conclusion

La lutte contre la piraterie frauduleuse renvoie ainsi à la question de la sécurité des États et montre toute la complexité des enjeux géopolitiques de la cyberpiraterie. La cyberpiraterie de renseignement et les actes de cyberguerre ne se produisent pas indépendamment des rivalités de pouvoir terrestres entre États et forces politiques mais ils ajoutent une dimension supplémentaire à ces conflits, dont les formes d'expression sont radicalement nouvelles, complexes à appréhender et déstabilisantes.

Peut-on encore penser la cyberpiraterie en la visualisant à travers nos schémas cognitifs classiques ? Si le cyberespace est un espace de pouvoir comme d'autres (la terre, la mer, l'air, l'espace stratosphérique), comment peut-on rendre compte de la répartition de la puissance en son sein ? C'est là un problème que la géopolitique se doit d'aborder.

Bibliographie

BARLOW J. P. (1996) « A Declaration of the Independence of Cyberspace » http ://homes.eff.org/barlow/Declaration-Final.html.

CHINA ECONOMIC AND SECURITY REVIEW COMMISSION (2008), « Report to the Congress of the U. S. », 110e congrès, 2e session, novembre.

HODGE N. (2009), « Inside Moldova's Twitter Revolution », Danger Room, 8 avril, http ://www.wired.com/dangerroom/2009/04/inside-moldovas.

INFORMATION WARFARE MONITOR (2009), « Tracking GhostNet : investigating a cyberespionnage network », 29 mars, University of Toronto, Canada.

KRAMER F. D., STARR S. H., WENTZ L. (2009), *Cyberpower and National Security*, NDU Press, Washington.

OWENS W. A., DAM K. W., LIN HERBERT S. (2009), « Technology, policy, law, and ethics regarding U.S. acquisition and use of cyberattack capabilities », Committee on Offensive Information Warfare, National Research Council, Washington D.C.

Security Labs : http ://securitylabs.websense.com/content/spamPercentage.aspx