

10 - INTERNET GOUVERNANCE ET ACTEURS

Constatant l'importance d'internet et de ses applications, nous avons consacré cette année trois chapitres à ce sujet. Voici le premier, qui traite des acteurs institutionnels (Icann, W3C) et des grandes manœuvres des entreprises du secteur. Cette année, ce sont les moteurs de recherche qui ont retenu notre attention.

Actualité 2003 des noms de domaine : une année de transition

Patrick Maigron

Une année assez calme dans l'actualité des noms de domaine, rythmée par la libéralisation progressive des extensions nationales et la mise en œuvre attendue des noms internationaux et de l'extension européenne. L'événement le plus marquant aura probablement été l'affaire « Site Finder », véritable pavé dans la mare déjà fort agitée de la gouvernance Internet¹.

En janvier, l'extension .ORG est passée sans encombre des mains de Verisign à celles du nouveau registre PIR, émanation de l'Internet Society. Le suffixe .PRO consacré aux professions libérales s'est ouvert en juillet, et le sous-domaine .KIDS.US aux jeunes Américains en septembre. Le domaine européen .EU sera finalement géré par Eurid, consortium regroupant les registres belge, italien et suédois. Il s'agira d'un modèle d'enregistrement ouvert (premier arrivé – premier servi), réservé cependant aux ressortissants de l'Union européenne. Le lancement a pris beaucoup de retard, les règles de fonctionnement devant être ratifiées par les Etats-Membres, il est désormais prévu pour novembre 2004. Les arnaques à la pré-réservation se multiplient entre-temps.

Devant la relative stagnation des enregistrements, de nombreux registres nationaux adoptent des modèles plus ouverts, en prévision des nécessaires investissements à venir (noms internationaux, IPv6, ENUM) et de la concurrence du .EU. C'est le cas des pays suivants : Pays-Bas, Turkménistan, Chine, Suède, Finlande, Corée, Equateur et Espagne tout au long de l'année. On observe ainsi une harmonisation des modèles d'enregistrement : noms libres sans vérification préalable, procédures automatisées peu coûteuses et vérifications *a posteriori* seulement en cas de litiges. Même le registre français, très attaché à la notion de « domaine de confiance », prépare sa

¹ Voir encadré à la fin de cette section

L'année des TIC 2003 :

Télécom - Electronique - Informatique - Médias - Internet

mini révolution pour mi-2004 : supprimer le droit au nom (aujourd'hui les noms doivent être alignés sur les patronymes, les noms de marques ou les raisons sociales). La restriction de territorialité et l'identification systématique du demandeur demeurent cependant.

Les noms de domaine internationaux utiliseront finalement la nouvelle technologie IETF normalisée fin 2002 au lieu de celle déjà expérimentée par Verisign. L'objectif était de ne pas modifier le système DNS et de ne toucher que les applications (agents de messagerie, navigateurs web). Ainsi une société française enregistrant le nom «café.fr » se verra-t-elle attribuer dans les serveurs DNS la séquence « xn--caf-dma.fr » (le préfixe « xn-- »² indiquant un nom international et « -dma » le caractère « é »), les applications se chargeant de la traduction visuelle en caractères accentués. Plusieurs registres proposeront des caractères nationaux prochainement : .INFO fin 2003 (seulement 3 caractères : ä, ö, ü), le Danemark en janvier 2004, l'Allemagne, l'Autriche et la Suisse en mars suite à un travail commun (92 caractères accentués), la Corée et le Japon... Devraient suivre d'autres registres asiatiques, ainsi que .COM/.NET/.ORG.

Du neuf aussi du côté de l'Icann qui a signé en septembre son sixième contrat avec le Département du Commerce américain : un nouveau président Paul Twomey (australien, homme de communication et fin politicien), un premier bureau international en Belgique, un nouveau site web bientôt multi-lingue et de nouveaux dossiers en cours sur la création de nouvelles extensions génériques et la sécurisation du DNS... Et tout ça n'a pas suffi à calmer les esprits et à empêcher la création d'un groupe de travail sur l'évolution de la gouvernance d'Internet lors du SMSI !

² Ne cherchez pas un acronyme dans le préfixe « xn ». Celui-ci a été choisi parmi les séquences de deux lettres qui ne sont pas déjà des codes de pays, au moyen d'un tirage pseudo-aléatoire conçu également par l'IETF et basé sur les volumes d'échange de 12 actions (6 NYSE, 6 NASDAQ) relevées le 10 février. Tiens, pourquoi seulement la bourse de New York ?

L'affaire *Site Finder*

Le 15 septembre, Verisign lance sans préavis un nouveau service baptisé *Site Finder*, basé sur la technique des jokers dans les zones COM et NET. Ce service permet de capturer les fautes de frappe dans les requêtes web émises par les internautes, et de les rediriger vers une page de Verisign proposant des suggestions ainsi qu'un moteur de recherche et des liens sponsorisés. Verisign met en avant la volonté d'aider les internautes, mais les liens sponsorisés constituent la véritable justification financière de l'opération (il y aurait 20 millions de fautes de frappe chaque jour sur ces deux domaines).

Ce service engendre immédiatement un tollé de la communauté internet, condamnant cet « abus de position dominante ». Tour à tour, le comité représentant les utilisateurs et le comité sur la sécurité et la stabilité de l'ICANN, l'instance de standardisation IAB, mais aussi l'AFNIC et le CIGREF en France recommandent la suppression du service. Trois procès au moins se préparent contre Verisign, et les pétitions en ligne d'internautes se multiplient. Des contre-mesures techniques voient également le jour : modification des logiciels DNS pour filtrer ce service et mise en œuvre du filtrage par les FAI.

Le 19 septembre, l'Icann *demande* à Verisign de suspendre son service, dans l'attente des résultats d'une étude sur ses conséquences techniques ; Verisign refuse. Le 3 octobre, l'Icann *somme* Verisign de le fermer sous peine de remettre en question le contrat qui lie les deux parties ; Verisign cette fois-ci obtempère. Mais n'en reste pas là pour autant... Le 7 octobre, Verisign publie ses réponses techniques aux objections de l'IAB, concluant que *Site Finder* ne cause aucun problème de sécurité, ainsi que le résultat d'une étude de satisfaction selon laquelle 84 % des internautes préféreraient ce service à la page d'erreur standard des navigateurs. Le 15 octobre, la société annonce qu'elle relancera le service après quelques corrections mineures, cette fois-ci avec un préavis d'un mois. Et le lendemain, son PDG passe à l'offensive en suggérant un changement de statut de l'Icann et un rôle accru du secteur privé dans la gestion de l'Internet.

Ce même jour, Verisign annonce qu'elle vendra en fin d'année à un fonds d'investissement sa filiale Network Solutions, chargée de la fonction très concurrentielle de bureau d'enregistrement de noms, la maison mère conservant la fonction principale de registre. Cette séparation entre les activités de détaillant et de grossiste est une décision positive réclamée depuis bien longtemps, mais certains analystes y voient une possible monnaie d'échange pour un assouplissement des décisions concernant *Site Finder*...

Moteurs de recherche

Michel Berne

La Toile étant depuis longtemps immense, on a besoin de guides pour s'y repérer. Et le meilleur de ces guides va prendre le dessus et écraser ses concurrents. 2003 a été riche en grandes manœuvres dans ce domaine.

Tous les portails, utilisent les moteurs de recherche pour les quelques 550 millions de requêtes décomptées quotidiennement sur le web. Ainsi mi-2003, MSN utilisait le moteur d'Overture et Yahoo!, comme AOL, le moteur Google. Google était également disponible sur son propre site qui n'offrait que de la recherche « pure ».

La qualité d'un moteur de recherche dépend de deux facteurs : le nombre de pages cataloguées et la capacité à présenter les pages pertinentes suite à une requête. En 2003, un moteur comme Google indexant de l'ordre de trois milliards de pages, on voit donc que le problème est vraiment crucial. De plus, l'ordre dans lequel les pages apparaissent à l'écran joue un grand rôle dans leur visibilité, car aucun internaute, même très obstiné, ne va explorer des dizaines de milliers de référence. Enfin, il faut que ce service gagne de l'argent. La publicité, la vente de services annexes et aujourd'hui aussi le référencement payant des sites les plus visibles sont trois possibilités. Ainsi Overture (propriétaire des moteurs Altavista et Fast) vend aux enchères des mots, qui sont alors associés à des adresses de sites. Ces sites paient Overture lorsque l'internaute clique sur leur adresse.

Les liens payants exigent un peu de doigté dans leur mise en place. Les internautes américains qui cherchaient avec Google des informations sur un fait divers tragique - un cadavre découpé en morceaux et retrouvé dans une valise - se sont vus proposer des publicités pour les bagages.

Yahoo!, le site « historique » de la recherche, tire ses revenus de multiples services. Mais le site Google attirait de plus en plus de visiteurs (sa part de marché mondiale étant passée de 1 % en 2000 à 40 % environ en 2003). Yahoo! a donc décidé de réagir en achetant successivement le moteur Inktomi et surtout Overture en juillet 2003 pour 1,6 milliard de dollars (Overture assurait déjà la gestion des liens promotionnels de Yahoo!). De son côté Google a racheté Applied Semantics et Blogger.com, lancé des revues de presse et un comparateur de prix (Froogle, fin 2002). L'entreprise devrait s'introduire en bourse en 2004.

L'année des TIC 2003 :

Télécom - Electronique - Informatique - Médias - Internet

En dehors des problèmes de stratégies d'acteurs, il y a deux points délicats. Le principal porte sur la qualité du service rendu. Quelle confiance accorder à un moteur qui place en tête de liste systématiquement (et de manière parfois invisible pour l'internaute) les liens « sponsorisés » par des annonceurs ? Les grands moteurs disent faire clairement la distinction entre ces derniers et les autres. Mais comme ils reçoivent des annonceurs de 15 à 75 US cents par lien cliqué, la tentation est grande de faire pression sur ces derniers pour qu'ils paient leur référencement. Par ailleurs, les algorithmes utilisés par les moteurs pour classer les pages par ordre de pertinence sont peu transparents et évoluent vite. Ainsi, le moteur Dipsie, qui devrait être actif mi-2004, indexera 10 milliards de pages, incorporera des outils sémantiques améliorés et indexera les pages dynamiques. De son côté, Microsoft aurait mis 200 ingénieurs au travail dans ce domaine.

La présentation des résultats évolue aussi. A côté de la traditionnelle liste, on trouve des systèmes graphiques sous forme de cartes ou d'arbres (Kartoo, Grokker ou encore Mindmanager³).

Les mots les plus populaires sur les moteurs de recherche dépendent du portail. *Le Journal du Net* synthétise ces demandes pour les principaux moteurs en France. Dans le bilan 2003 qu'il a publié, les utilisateurs de Lycos se distinguent par leur intérêt pour le sexe. Ailleurs, sur MSN, Google, Yahoo! et AOL, les questions pratiques dominent : SNCF, annuaire, ANPE, météo. Star Academy et Matrix font partie des cinq premières requêtes sur Google alors que Kazaa occupe la 3^{ème} place chez AOL.

Source : <http://www.journaldunet.com>

W3C

Dossier préparé par un groupe d'étudiants de l'option projets audiovisuels-multimédia de l'INT et mis en forme par Michel Berne

Le W3C, le *World wide web consortium* a en charge la normalisation de la toile. Créé en 1994, c'est une organisation internationale qui compte plus de 450 membres. Il est dirigé par Tim Berners-Lee, l'inventeur du web tel que nous le connaissons aujourd'hui. Le principal problème du

³ <http://www.kartoo.com>, <http://www.groxis.com>, <http://www.mindjet.com>

Lire sur le sujet des interfaces : Ben Shneiderman, *Leonardo's Laptop*, MIT Press, 2002.

L'année des TIC 2003 :

Télécom - Electronique - Informatique - Médias - Internet

W3C est de gérer la croissance explosive du web, non pas tant en nombre d'utilisateurs, mais en développant de nouvelles technologies pour qu'on en tire le plein potentiel.

Sept points-clés résument les ambitions du W3C :

- Accès universel : le W3C prend des initiatives pour assurer que toutes les informations accessibles sur un réseau soient accessibles depuis toutes sortes de machines et en tout lieu ;
- Web sémantique : comment introduire du sens, interprétable par les ordinateurs, dans les contenus sur le web pour faciliter la recherche d'information, la traduction entre langues et plus généralement l'activité humaine. Le développement des langages de la famille XML en forme le premier pas ;
- Confiance : authentification et sécurité des messages et des transactions ;
- Intéropérabilité : une nécessité compte tenu de la complexité et de l'utilité croissantes du web ;
- Capacité à évoluer : lié au point précédent ;
- Décentralisation : idem ;
- Multimédia : pour intégrer des contenus multimédias au web ; développement de langages comme SMIL ou SVG.

La tâche est donc immense et, compte tenu de son caractère non-gouvernemental, le W3C ne peut compter que sur son autorité morale et sur le consensus de ses membres pour réussir. Il n'est donc pas étonnant que plusieurs dossiers se révèlent sensibles.

Le premier porte sur l'évolution du langage « historique » du web, le HTML. Empêcher que des sous-normes privées ne détruisent l'interopérabilité a été un souci constant du W3C, avec d'un côté des acteurs qui freinent le mouvement et de l'autre des industriels qui l'accélèrent et éventuellement introduisent leurs propres variantes. Le deuxième dossier porte sur le conflit traditionnel entre systèmes propriétaires et libres. Le W3C a publié en mai 2003 après un long débat son Règlement des brevets, qui confirme que les normes du web devaient être libres de droit. Le dernier dossier enfin porte sur la capacité du W3C à fédérer tous les grands acteurs du monde du web. Le W3C est trop grand, trop lent, trop mou pour des géants comme Microsoft qui pensent que leurs intérêts commerciaux seraient mieux défendus dans une structure comme OASIS regroupant les grands industriels. Ainsi la normalisation des *web services* pourrait largement échapper au W3C et se faire dans le cadre d'OASIS. Microsoft a d'ailleurs quitté le groupe de travail *web services* du W3C.



Les documents de ce site sont sous [Creative Commons License](#)



N.B.

Spam spam spam spam and spam

Nigel Barnett

It has choked off newsgroups, clogged blogs and blocked mailboxes. Spam is not going to go away. It has become a serious and costly nuisance but there are signs that major Internet players are fighting back.

The Empires strike back

The proliferation of Spam on the internet or UCE, unsolicited commercial email, has once again been centre stage in 2003.⁴ In the UK a Spam Summit took place in July as a result of an inquiry by a parliamentary Internet group and in France in November the first National Spam Forum attracted over 250 professionals and interested parties to the National Assembly to discuss the problem and share experiences. At an international level, European directives to establish a legal framework to combat spam have already been adopted in some EU countries but by no means in all. In the United States, after being under pressure from legal initiatives emanating from individual state legislatures, the American Senate finally passed the Can Spam Act. This law makes the sending of bulk mail by companies or individuals who do not respect certain criteria illegal. The bill also sets up a 'Do Not Mail' registry for those who wish not to receive email marketing, a system similar to the 'Do Not Call' list managed by the Federal Communication Commission which is designed to protect people from telemarketing. Other measures have been instigated by Internet Service Providers who are right in the firing line; AOL admits to blocking as many as 2.4 billion suspected spams a day on their networks. In June 2003 Microsoft filed 15 suits against spammers suspected of sending more than 2 billion spam messages to MSN and Hotmail users in the US and the UK. In December New York's Attorney General in association with Microsoft went gunning for a whole gang of spammers seeking over \$38 million in reparation. California and Virginia also indicted individual spammers using their existing laws. In France, despite the CNIL going on the offensive, only a couple of small spammers have been convicted and the transposition of the European directive on E-Privacy, which provides a legal framework for attacking spammers, seems stalled.

Spam viruses and fraud on the increase

Meanwhile companies and individuals continue to suffer. According to Brightmail an anti-spam specialist, more than half of the mail sent over the Internet is spam and a spammer will typically send up to 200 million messages a day of which 85% originates in the United States. The trend in 2003 has been the increasing cleverness of the spammers in making their messages

⁴ For more background see last year's article and the year before!

L'année des TIC 2003 :

Télécom - Electronique - Informatique - Médias - Internet

resemble valid email thus increase the likelihood of them being read by unsuspecting mail users - while avoiding the more and more sophisticated filters employed by anti spam software providers like Brightmail and its rival Message Labs. Just to make matters worse virus creators have been borrowing techniques from spammers to promote their exploits with the result that the Sobig virus was able to become the most successful virus worm ever (see article SoBig So Bad).

With regard to spam content, the traditional links to pornographic and financial service sites remain 'popular', but it is the growth of fraudulent email that has marked 2003. Through social engineering techniques it has got much slicker and there is a growing use of 'spoofing' and identity 'phishing' which gives the impression to the credulous Internet user that the message seems to be from well-known legitimate companies such as banks and online auctioneers.⁵ False login pages then encourage the internet user to enter personal account numbers, confidential codes and passwords. It only takes a few gullible users to make the scam pay.

La compagnie Hormel qui produit le célèbre pâté de viande SPAM attaque en justice une société qui vend des produits anti-spam et veut utiliser le mot « Spam » dans une marque qu'elle a déposée.

Companies count the cost

The cost of fighting spam at a corporate and institutional level is difficult to estimate precisely. Message Labs have calculated that UK companies lost €4.6b in earnings in 2002 because of spam and US companies double that in 2003. A well-known British University spent €14,000 on spam filtering software plus €1.6m a year implementing it. According to Ferris Research it costs companies who do not have email filtering \$168 per mailbox per year, almost three times as much as the combined costs of licenses, running costs and lost earnings from false positives associated with mail filters. Spam filters, however sophisticated they are, are by no means perfect. They are reactive rather than proactive and spammers are able to get round most filters one way or another. The wholesale blocking of suspect mailings, a strategy employed by ISPs is not without risk for companies either. They may find themselves falsely blacklisted by anti-spam blocking and once again suffer loss of earnings or even go out of business. Perversely the most handicapped companies will be the direct marketing profession who will find themselves burdened by more rules and regulations and the threat of heavy fines, particularly in Europe, if they stray from the straight and narrow, while spammers around the world continue with relative impunity. Mail shots will have to be accomplished with almost surgical precision and records of all communications backed up solidly!

⁵ Now at 10% of email Spam, according to BrightMail.

Opt in Opt out

Will the authorities armed by new legislation make an impression on the deluge of spam in inboxes around the world? The answer is no! At least not in the short term, spammers are not law abiding citizens in general and although a few may be dissuaded from continuing, the absence of any global solution will allow the majority to evade effective control. The problem of co-operation is illustrated in the important cultural differences that were observed between the approach adopted by the United States and that of Europe. For many experts in Europe the American *opt out* choice is a *license to spam* for marketers. By the time you tell a company that you do not wish to receive their unsolicited email you have already had it. They also doubt the effectiveness of the 'Do Not Mail' register. For the United States the priorities have been put on the honesty of the message in terms of its origin and content while preserving the rights of free expression. By insisting on an *opt in* approach Europe emphasises the right to privacy and is particularly concerned with how personal information like email addresses are collected and used.

No quick fix in sight

While the idea of making email a progressively paying service (where the cost increases with the number of mail that are sent) is an attractive one at first sight, putting such a scheme into practice would be a daunting task. It is unlikely that anything other than a complete revision of the Simple Mail Transfer Protocol, SMTP protocol will have any effect. This is because the protocol is fundamentally flawed. It was simply not designed to be secure nor does it offer any sort of effective authentication procedure. Changes at such a fundamental level require a great deal of consultation and this is exactly what the Anti-Spam Research Group (ASRG) of the Internet Research Task Force (IRTF) is attempting to do.⁶ Of course technical change is essential but only a concerted effort at all levels will have any lasting effect on spam. It may be that solutions will come too late to save email and that the economic theory of the '*tragedy of the commons*', where a shared resource is destroyed by the lack of entry barriers or an effective regulatory authority will have found a new and exemplary, case study.

En mai 2003, le Tribunal de grande instance de Paris a condamné en référé l'organisation Droite Libre qui avait demandé à ses membres de bloquer sous les envois de courriels les sites des organisations syndicales pour protester contre les grèves dans les transports.

⁶ Website at <http://asrg.sp.am/> . For an excellent guide to spam prevention <http://spamlinks.port5.com/prevent.htm>. In French the guide put together by Frédéric Aoun et Bruno Rasle for the Spamforum in Paris is particularly comprehensive. http://www.spamforumparis.org/docs/Actions_a_mener.pdf

SoBig So Bad.

Nigel Barnett

Over 7000 new viruses were recognised in 2003 but none spread with the speed and the ferociousness of the *Sobig-F worm*, which hit homes and servers in August and made this month the worst ever in virus history. According to Postini the virus worm managed to infect more than 16 million machines and almost 4% of all email exchanges at one point. Its 'success' stems largely from a succession of techniques employed by the developers to replicate and spread the worm. Called *blended* threats by experts Symantec, the incorporation of spamming techniques in the proliferation process has led some experts to think that there has been collaboration between spammers and virus developers. Whether this collusion is real or imagined is of little concern however to the millions of people infected by viruses and inundated by spam. Evidence suggests that the worm was elaborated over a period of time, each variation from SoBig-A to SoBig-F adding an 'improved' blend of techniques.

More generally Sobig and other worms like Blaster and Sapphire caused a great deal of grief to Microsoft users, as all the major viruses targeted security weaknesses on Microsoft systems. The hijacking of unprotected computers by viruses using Trojan horse programmes has meant that they could then be used to turn them into spam engines not only to propagate the worm but also potentially to extract confidential data about the user. There seems to be no easy fix to the proliferation of virus/ worm/mass-mailers in sight. Virus makers are exploiting security loopholes more quickly according to Symantec and by the time the anti-virus companies have identified a virus, profiled it and made a fix available it is already too late for the most successful viruses to be contained. Companies have an increasingly difficult and expensive task ahead of them because the slightest breach in security may let in disaster

Similarly life is not going to become any easier for the average internet user who – enticed by new file sharing programmes, Internet phoning or instant messaging possibilities – is becoming increasingly vulnerable to attack from aggressive marketing, spyware and the more dangerous malware, malicious code that can be activated by third parties. Broadband 'always on' access can mean that users are unwittingly allowing their machines to be used by others in the code jungle that the Internet has become.

Des « virus-antidotes » existent. Ainsi Welchia éradique Blaster, mais encombre les réseaux. Le coût des virus pour les entreprises dans le monde est estimé par Trend Micro à 55 milliards de dollars en 2003 (seulement 13 milliards en 2002). Mais si la réalité de la croissance des dégâts n'est pas mise en doute, leur estimation financière est très délicate et dépend beaucoup de la méthodologie retenue.