

Internet, le choix :
consortium dot-root

**conduire maintenant,
s'unir rapidement
ou reconquérir lentement**

Chacun comprend que les réseaux de transmission de données publics (Internet, Minitel, Rita, Transpac, SITA, Swift, etc.) soient devenus fondamentaux à notre mode de vie actuel. Chacun peut comprendre que sans eux, notre économie, nos relations humaines, nos emplois, notre vie culturelle, notre santé, notre enseignement, notre information, notre défense, notre futur seraient rapidement et très gravement compromis. Chacun peut ainsi mesurer que leur contrôle et leur protection soient devenus des objectifs stratégiques, que leur maîtrise relève de la souveraineté nationale, que leur développement soit nécessaire au développement durable, et que la paix mondiale puisse dépendre, tant de la réduction de la fracture numérique que des équilibres et de la concertation trouvée dans leur gestion internationale.

Le 11 septembre 2001

Après le 11 septembre la Maison Blanche a demandé un rapport sur l'état et la sécurité de ces réseaux. Ce rapport est paru le 15 septembre dernier. Il est très clair : ces réseaux dominés par la technologie Internet (TCP/IP) sont une passoire où l'insécurité se développe à une vitesse que l'on pourrait qualifier de plus que rapide.

Cette insécurité permet la prise de contrôle via le réseau des systèmes informatiques (piratage), leur destruction (virus) ou leur saturation (DoS). Elle met gravement en péril l'infrastructure locale, régionale, nationale et globale des Etats Unis dans les domaines les plus divers, allant des transports, aux systèmes bancaires, en passant par la défense nationale, la protection des biens et des personnes, la formation et la santé. A la clé il y a des milliers, voire des millions de vies en jeu, potentiellement dans la minute : une menace de niveau nucléaire, sans possibilité de parade puisque le système électrique, les médias, les urgences médicales, la navigation aérienne, etc. en dépendent. Il cite des exemples de situations réelles accidentelles, pirates, ludiques, criminelles ou terroristes réellement advenues, et montre que leur succès ou leur conjonction catastrophique ne sont manifestement qu'une question de temps.

Cette présentation se fait toutefois, selon une vision fondée sur une logique et une réflexion anglo-saxonne des réseaux, exacerbée par le souci actuel de protection du "Homeland" nord-américain, où le territoire national inviolable est le centre du monde, protégé par un glacis où se passe la confrontation. Purement informatique, elle traite peu des raisons de la menace et donc de sa prévention "chirurgicale": toutefois des propositions privées parallèles, à but non-lucratif ou commercial, se font jour, qui participent de la même approche, ou du même marché.

Cette doctrine traditionnelle simple est maintenant confrontée à la violation territoriale du 11 septembre et au caractère virtuel du "champ de bataille" : il n'y a plus de sanctuaire. Le "core" de leurs systèmes informatiques est en prise directe avec l'agresseur (comme un château fort qui n'aurait pas de douves).

Il leur reste donc à prendre la pleine mesure de la globalité de la menace (un e-terroriste n'accédera pas nécessairement Internet à partir de Chicago, comme un pirate de l'air doit le faire). Ceci aura des implications de politique étrangère importantes que mesure manifestement l'auteur du rapport. Il semble qu'il se réserve les deux mois à venir pour se faire imposer par l'opinion démocratique (à travers une série de meetings dans les grandes villes), le besoin d'une défense globale contre un danger global. L'Iraq tombe (?) à point nommé comme exemple de risque distant; il sert ainsi de cas d'école pour une méthodologie de la prévention globale d'Etat.

La sécurité de l'Internet

Cette évaluation est exacte, mais pour bien l'analyser, il faut comprendre que l'Internet n'est pas un réseau structuré ayant sa sécurité propre, comme le téléphone, Transpac ou Swift.

Internet est un club ouvert à tout ordinateur s'interconnectant librement. Il est géré sous la forme de deux annuaires : les numéros des machines (adresses IP) et les noms des applications qu'ils hébergent (DNS, le système des noms de domaines).

Il est d'ailleurs défini comme tel par la loi des Etats-Unis (code des Communications – 47 USC 230 (f) (1)) : "le réseau informatique international des réseaux tant fédéraux que non fédéraux interopérables sous commutation de paquets". Ceci a la particularité de placer l'ensemble de l'Internet mondial – aux yeux de la législation américaine – sous la juridiction du Congrès.

Une bonne image est celle d'une ville champignon mondiale dont les immeubles sont référencés par des coordonnées attribuées au fil du développement (Adresses IP) et les habitants connus par leur pseudonyme (nom de domaine). L'on comprend que rien ne puisse s'y faire sans un plan numéroté des immeubles et d'un annuaire des pseudonymes. L'on comprend aussi que celui qui en voudra le contrôle expliquera qu'il apporte l'information, la stabilité et la sécurité mais à besoin d'exclusivité pour éviter la confusion.

C'est le cas, en particulier via la gestion des noms (système DNS) qui permet une gestion ou un blocage dynamique quasi-absolu des accès (par exemple, pour un e-embargo sur l'Irak non voté par l'ONU). La sécurité et la stabilité du réseau, l'internationalisation de l'usage, la protection des marques commerciales dans le nommage Internet, la rentabilité commerciales des entreprises clé qui le cogèrent, et surtout le contrôle politique qui en résulte, font de ce DNS le cœur des préoccupations du gouvernement nord-américain. Elles sont administrées par une société non-commerciale, sans membre, de droit californien : l'ICANN. Les gouvernements étrangers y ont seulement une capacité de conseil à travers le GAC (Conseil Consultatif des Gouvernements). Son vrai rôle, à travers un maillage de contrats complexes, auxquels se refusent la plus part des opérateurs nationaux et tous les Européens, est de concrétiser la doctrine, codifiée plus haut, d'une dominance des Etats Unis sur le réseau d'information mondial, dans un but d'efficacité, de paix, de justice, de stabilité (l'amendement connexe à l'article cité est dit "du bon Samaritain").

L'importance du nommage, des langues locales, et de ses retombées économiques, culturelles et sociales, le blocage de l'innovation technique et sociétale due à la sur-influence stratégique ainsi obtenue par les Etats-Unis, conduisent à des tensions grandissantes. Ces tensions ne pourraient que s'accroître si, comme le laisse entendre le rapport de la Maison Blanche, le DNS et les protocoles d'accès devaient être revus unilatéralement par le projet nord-américain. Ces tensions ne pourraient que s'exacerber si les compromis trouvés résultaient d'un manque d'information technique ou sociétale ménagé aux négociateurs.

Il y a trois orientations possibles pour la sécurité du DNS : la centralisation actuelle qui est la plus vulnérable mais la plus avantageuse pour les Etats-Unis; le cloisonnement par zone géographiques, qui réduit les risques globaux mais augmente les contraintes et laisse chaque partition vulnérable; la duplication de plusieurs systèmes parallèle opérant en contrôle mutuel, qui réduit les risques au maximum sans contrainte pour les utilisateurs, et permet, de leur fournir des avantages sélectifs.

Il est important que cette troisième architecture se mette en place peu à peu car elle permettra, de façon naturelle et sans opposition, sauf si elle était organisée sous la seule direction de l'ICANN, un rééquilibrage de la gouvernance du DNS et de l'Internet, dans la concertation.

Le plan de la Maison Blanche et nous

Le plan de la Maison Blanche que propose Richard Clarke est simple : prendre les moyens nécessaires pour sécuriser les Etats-Unis et ses ordinateurs, et de le faire. C'est la formule "un problème est fait pour être résolu" appliquée au premier degré.

La manière proposée est certainement adéquate : la coordination fédérale de l'effort des forces économiques qui sont directement menacées ou qui peuvent tirer un large profit de la réponse qu'elles développeront. L'on travaillera à défendre sa peau, celle de sa famille et des siens, à préserver son mode de vie, et l'on paiera ou l'on fera gagner l'argent qu'il faudra pour y parvenir.

Ce plan n'est ni altruiste ni généreux. Ce n'est pas un plan Marshall d'après guerre : c'est un plan de défense des Etats-Unis. Le réseau est mondial. Nous (les étrangers) ne sommes cités que comme des sources d'idées à ne pas négliger; ou comme une menace potentielle par notre désorganisation. L'Union Internationale des Télécommunications (UIT) est citée, mais l'on comprend qu'elle est d'abord un moyen pour de nous coordonner et de nous gérer, comme l'est aussi le GAC, le comité consultatif gouvernemental au sein de l'ICANN, qui n'a aucun pouvoir sur le DNS. Nos ressources, nos chercheurs sont souhaités au sein des équipes de R&D de l'Internet, mais nos Etats ne sont pas les partenaires du travail à entreprendre. Nos intérêts ne sont pas considérés : l'international qui est traité est celui des intérêts des Etats-Unis à travers le monde (l'Afrique n'y est pas citée).

Nous ne sommes pas dans l'arche de Noé.

Ne nous leurrions pas, même si une offensive de charme se développait vers nous : nous ne sommes pas dans l'arche de Noé, mais nos idées, nos produits devraient y être. Outre qu'il s'agit à la fois du "containement" et du protectionnisme américains (et républicains) traditionnels, il s'y ajoute un contexte d'urgence à l'obtention de contrats et de l'attention du marché qui rend difficile le traitement des coopérations internationales dans le cadre d'aides publiques ou privées et de projets sensibles voire qualifié de défense nationale.

Il suffit de lire ses spams quotidiens pour comprendre que la Sécurité Cyberspatiale va devenir une vache à lait. Qui voudrait se protéger "des risques venus d'ailleurs" en utilisant des produits "venus d'ailleurs", "home made" sera la première garantie dans de tels cas.

Il convient donc d'informer nos entreprises. Il leur sera, en effet, très difficile de faire valoir les droits d'accords mal protégés lorsque le produit résultant sera classé "Homeland protection". Il faut aussi souligner que le risque est universel, et donc le marché également Européen.

Nos options

Nous nous trouvons donc à une croisée des chemins.

1. ou nous laissons faire, et la technologie Internet sera totalement revue, professionnalisée, sécurisée par des laboratoires de recherches nord-américains sous contrats fédéraux, exploitant la coopération de nos propres chercheurs à travers les structures techniques communautaires de l'ISOC (Internet Society) où le poids et l'historicité américains sont très naturellement importants. Des licences s'appliqueront de plus en plus, pour des raisons objectivement sécuritaires mais aussi commerciales. Le leit-motiv du "parapluie commun" s'appliquera à nouveau : "nous nous protégeons, nous pouvons aussi vous protéger, mais selon nos solutions. Après tout le Net c'est nous qui l'avons développé".

Ceci conduira à un réseau à deux vitesses : "Nord" dépendant fortement des USA, "Sud" en GPL peu compatible et ouvert; avec tous les déséquilibres, les vindictes et les instabilités qui en résulteront et ne profiteront à personne. Le "digital divide" deviendra le "digital gap".

Nous devons alors relancer une stratégie d'autonomie comparable à l'autonomie nucléaire car nous sommes là sur un même registre mondial et d'enjeux économiques et militaires, mais aussi ici sociétaux fondamentaux.

2. ou nous disons, et surtout nous faisons en sorte, que cette révision technique - qui est nécessaire - soit universelle. Cela signifie qu'elle soit non seulement engagée avec nous, mais encore qu'elle soit ouverte à tous..

Certes, nous nous assurerons ainsi que la dominance nord-américaine ne nous place pas en situation de dépendance et que nous aurons nous aussi accès au marché mondial dans les mêmes termes. Mais nous assurons aussi d'une concertation responsable qui permettra de meilleures stabilité, sécurité et innovations.

Souvenons-nous que c'est Louis Pouzin et l'INRIA qui ont apporté les zones de l'Internet, le protocole qui le fiabilise, voire un budget à un moment critique initial. Souvenons-nous que nous avons créé le nommage ensemble (Europe et Etats-Unis), que Transpac et le Minitel sont français, le Vidéotex européen, que l'ISO résulte des travaux de l'IUT, que l'Internet ne résulte en fait que du choix de l'Anglais Berner-Lee pour son application "web" du CERN.

Souvenons-nous surtout ...

... qu'à réseau global, il faut nécessairement un effort de développement global.

Nous ne désirons être ni des ennemis, ni des troupes auxiliaires; ni des clients achetant leur sécurité. Nous désirons être les partenaires d'un e-OTAN dont la mission sera, selon l'heureuse formule de G.W. Bush, de défendre, de préserver et d'étendre la paix. Mais une paix définie en commun, comme le lui réclamait le Maire d'Hiroshima. Une paix reposant sur l'expérience et les apports de chacun.

Les actions à mener

Pour cela nous devons mener trois types d'actions. Une action gouvernementale, un effort industriel et technique et une action au sein de la gouvernance de l'Internet.

L'action gouvernementale est engagée par les positions au sein du GAC, par les relations bilatérales, par l'Union Internationale des Télécommunications. Elle a déjà amené des résultats, mais nous sommes là dans les principes généraux et le moyen/long terme. Une fois l'Internet reconstruit par (ou mieux : avec) les Etats-Unis, SAIC, Verisign, Microsoft, AT&T, IBM et WorldCom, comment le gérerons-nous ? Il importe que nous soyons comptés parmi ces ténors de l'Internet, **au sein de la gouvernance**, pour qu'il y ait un consensus et un équilibre d'intérêts stable entre les grands acteurs. Nous devons voir nos entreprises compter parmi ceux que la "communauté ICANN" nomme les "stakeholders".

Un effort industriel et technique brusque est difficile à gérer pour notre planification européenne. L'infrastructure de l'Internet est légère. Elle est dominée par des sociétés nord-américaines, dont Cisco et sans doute un jour Microsoft, déjà allié à Verisign pour son effort sur les noms de domaines multilingues, vers l'Asie, puis vers l'Europe. Un déploiement industriel et télécom particulier semble difficile dans ce contexte ? Il sort du cadre de la valeur ajoutée de l'Internet.

Par contre nous avons sans aucun doute un très fort potentiel dans les retombées industrielles d'applications nouvelles du réseau, qui seraient à notre initiative et rendues possibles par une action ad hoc **au sein de la gouvernance**. Par la "légitimité" du Minitel, un large champs d'action nous est en particulier ouvert dans le domaine de l'Internet de proximité et du téléurbanisme (Webs de France), des communautés entrepreneuriales, des web services, des outils de développement durable, des portails personnels (uPortal de l'Education Nationale) etc. C'est jouer là vers le PC virtuel (le "Supertel"), le système d'exploitation réseau, etc. nous plaçant directement en concurrence favorable avec Microsoft (Longhorn, Windows 2005).

Pour soutenir cette action politique, pour aider un effort industriel concerté, il nous faut participer à l'effort de la gouvernance "à la Internet", et même le conduire dans les domaines où nous sommes plus aptes à le faire. Pour cela il faut un projet acceptable, au cœur du système, qui soit **compréhensible, réaliste et concret** pour des gens qui se sentent en guerre, et qui se lancent dans un véritable projet "Manhattan II" ou "Apollo II".

Nous avons pour cela 8, 80 ou 8000 jours

8 jours, car les Etats-Unis ont engagé, très vite après le 11 septembre, l'action de réflexion et de préparation concernant leur structure de riposte. Ils ont donc pris, plus que nous, la mesure du danger d'une situation qui se dégrade rapidement. Ceci se traduit par les échéances "au pas de charge" d'un bouclage de leur dispositif, de la semaine prochaine à avant la fin de l'année.

8 jours pour co-conduire ce processus, 80 jours pour s'y unir ou 8000 jours pour reconquérir notre place si nous n'avons pu nous y associer à temps. Faisons donc le point.

Richard Clarke (M. CyberSécurité du "Homeland" et de la Maison Blanche) sait qu'il aura le soutien de chacun. Chacun peut en effet mesurer le taux des attaques que subit son propre PC dès qu'il se connecte : nous soutiendrons tous quiconque voudra lutter avec sérieux contre cette augmentation, non seulement de la menace, mais aussi de l'agression. Même s'il y avait là une part de dramatisation, cette dramatisation ne serait, qu'une composante de la situation telle qu'il nous faut la prendre en compte.

Le processus de redéploiement de la gouvernance de l'Internet est pratiquement terminé :

- Il passe par l'ICANN (organisme chargé par le gouvernement américain de privatiser/gérer sa participation dans l'Internet). L'adaptation de l'ICANN a été engagée en début d'année. Jusqu'à présent la stratégie de l'ICANN consistait à forcer la main aux Etats, en prenant des options pour tous les Etats qui auraient dû être prises par chacun d'entre eux, puis à leur proposer de normaliser par un accord mettant leur Internet sous la dépendance des Etats-Unis. Devant son insuccès, l'ICANN a clarifié les choses en leur demandant de la financer, avec peu mais quelques succès. Maintenant elle finit de se réformer pour gérer le "core" du réseau, le château-fort du "Homeland" : le DNS et ses aspects sociétaux. Cette réforme, largement contestée sera bouclée le 27 octobre, lors d'une réunion à Shanghai. Les modalités de la transition seront arrangées d'ici la fin de l'année, permettant une bonne coordination de toutes ces initiatives.
- Il passe par la finalisation du rapport CyberSpace Security de Richard Clarke, évoqué plus haut. Ceci se fera probablement pour la même date. La Maison Blanche animera une reprise en main totale de l'internet, conformément à la loi, sous le contrôle du Congrès. Les priorités sont le DNS et la sécurisation des protocoles d'accès, par-là de l'architecture des systèmes.
- Il passe par la stabilisation du DNS par "MicroSign" (surnom donné à l'accord entre Microsoft et Verisign, gestionnaire des ".com/.net") autour des noms de domaines "internationalisés". Ils visent là, grâce à une complexité technique, en partie artificielle, la prise en main du DNS en langues locales, et à la maîtrise de l'URL (la ligne de commande internet que chacun clique) qui est en passe de devenir peu à peu la "télécommande de notre quotidien".
- Il passe sans doute par le financement stable et important des structures de la dominance par le transfert à l'ISOC de la gestion du suffixe ".org", soit une prébende de 18 millions de dollars annuels qui arrivait à échéance. L'ISOC réunit les grands partenaires de l'Internet – principalement nord-américains – hors du contrôle des utilisateurs qui ne sont plus membres depuis cette année que de ses chapitres nationaux, et non plus de sa structure globale.
- il passe aussi par une sensibilisation importante du public nord-américain dans le cadre du "Homeland", de l'anti-terrorisme, de la vague morale contre les dirigeants escrocs qui ajoute sans aucun doute au sentiment d'insécurité et conditionne le marché domestique, et par son impact, le marché mondial. Cette sensibilisation associe fortement les professionnels à titre privé, par des questionnaires, des rencontres locales, etc. . Ceci donne à l'ensemble une base style logiciels libres qui ne pourra que l'asseoir solidement. Mais le public n'ira probablement que vers des solutions commerciales, bénéficiant d'un label et d'assurances.

Tout ceci créera des "avantages acquis pour les Etats-Unis" qui seront sans doute irréversibles avant très longtemps.

Les conséquences si nous ne réagissons pas

Si nous laissons le débat au seul plan politique et que nos projets industriels et logiciels, même très lourds et bien exportés, se conduisent sans notre participation significative au cœur du processus, c'est à dire au sein du tissu de la gouvernance qu'accapare l'ICANN, rien ne changera beaucoup dans notre vie de tous les jours. Mais ...

Nous serons peu à peu sous un contrôle pratique accru des Etats-Unis (y compris en terme de sécurité : la protection du "Homeland" est la priorité). L'accès à l'information sera de moins en moins partagé, sans doute un jour sous péréquation sociale mondiale contrôlée au moins en large partie pas Microsoft. Nous serons de plus en plus soumis à un profiling sécuritaire et commercial permanent, basé sur des données privées dont nous ne serons plus maîtres. Notre formation, notre santé, dépendra de plus en plus de solutions et de coûts que nous ne contrôlerons pas. Nous irons de plus en plus travailler dans les laboratoires développement sous une gestion centralisée aux Etats-Unis.

Nos lois et nos usages, notre politique étrangère, puis domestique, influencés par le moyen de leurs outils logiciels devront peu à peu se conformer aux décisions du Congrès. Bien des innovations techniques et sociales originales de la France (Minitel) et de l'Europe (subsidiarité) seront reléguées pour des décennies, jusqu'à être réinventées et sans doute nous être proposées un jour "sous licence".

Il y aura des difficultés accrues pour l'exception culturelle, la langue, la culture, ... Les schéma de notre vie locale, associative, familiale fortement dépendants des applications en réseau seront influencés : il y a deux ans 60% du trafic Web allait dans le monde vers 110 sites, cette année vers 16 seulement. Educause (administrateur d'un ".edu" devenu exclusivement nord-américain) délivrera nos diplômes de référence, comme le fait MS pour son informatique.

Les irritations personnelles, politiques et religieuses iront s'accroissant. Wall Street sera un peu plus le centre du monde au cœur de sa capitale virtuelle, et sans doute son centre de catastrophe - le 11/9 a montré ce qu'il en est, ou ce qu'il peut en être.

Tout cela continuera simplement une tendance que nous aimerions corriger et même améliorer dans l'intérêt commun par nos apports européens et l'enrichissement d'autres cultures, car de tels déséquilibres ne peuvent pas engendrer la stabilité.

Pouvons-nous le faire ?

Oui.

C'est même assez simple, car il ne s'agit pas de s'opposer à un effort technique majeur et nécessaire, mais d'y coopérer, de le co-animer, voire de le conduire dans l'intérêt commun là où notre compétence est reconnue, pour qu'il puisse trouver son équilibre et bénéficier à tous.

Cette réponse devra viendra un jour, car il n'est pas possible que toute la planète dépende même dans le moyen terme d'une pensée technique, légale, sociale, culturelle unique. Elle sera même probablement souhaitée un jour par nos amis américains. Mais aujourd'hui, ils sont confrontés à un problème grave et urgent, qu'ils s'estiment les seuls à avoir évalué, à vouloir, et donc à pouvoir traiter correctement. C'est d'abord un problème de leur sécurité nationale.

Pour nous, les questions sont le coût, la rapidité et la difficulté à définir et faire reconnaître notre participation, et ce qui se passera (ou ne se passera pas) avant qu'elle soit acceptée. Au cours d'un récent échange avec un responsable européen nous les avons évalués :

- avant le 20 octobre 2002 : gratuit, immédiat, de soi.
- avant le 31 décembre 2002 : cher, une ou plusieurs années, à négocier
- après : très cher; une dizaine d'années, à conquérir.

Ces dates résultent simplement de l'agenda américain très clair de leurs prises de décisions.

Il nous faut donc un ou des projets, centraux à l'Internet, engagés de longue date, pouvant être annoncés d'ici au 20 octobre et pleinement en opérations crédibles d'ici la fin de l'année.

En existe-t-il un ?

Oui. Il s'appelle "dot-root". Il est prêt. Il vise un impact fondamental sur l'Internet. Avec un peu d'aide il sera pleinement opérationnel et documenté le 20 octobre.

Lancé sur initiative privée, voire personnelle, il ne réclame pas qu'un portage urgent de mise en route de 10 à 30.000 euro et devrait ensuite pouvoir s'autofinancer.

la proposition dot-root

Le fonctionnement ordinaire de l'Internet repose sur le système de gestion de l'annuaire des noms de domaine (DNS) qui fournit la correspondance entre les noms de domaine et le numéro des ordinateurs où ils sont hébergés. Le cœur du DNS est constitué de 13 serveurs, fournis et opérés à titre bénévole. Leur rôle est de diffuser le premier niveau de cet annuaire : les numéros des serveurs offrant les annuaires des suffixes (".com", ".net" etc..).

Le document ICP-3 définit la doctrine de l'ICANN qui réclame l'exclusivité dans la gestion de ce système. C'est lui qui, par exemple, fait dépendre du Department of Commerce l'attribution et la mise en route du suffixe ".eu". Ce document indique que l'expérimentation par la communauté des utilisateurs est de la nature même de l'Internet. Qui plus est, il prévoit qu'une telle expérimentation pourra conduire à une gestion plurielle du système racine.

"dot-root" applique ce document et répond au besoin d'une telle expérimentation.

"dot-root" consiste en l'organisation bénévole au sein de la communauté des utilisateurs Internet d'un ensemble d'au moins trois systèmes de serveurs racine, opérés totalement en parallèle, pour l'étude, le développement, les validations, le déploiement et l'analyse en vraie grandeur de projets expérimentaux concernant le DNS, ses extensions et ses implications sociétales, à commencer par une gestion de systèmes racine parallèles, séparée et mutuellement contrôlée.

Cette plate-forme est déjà en pré-opérations. Elle se veut seulement un outil technique et social, à la disposition de tous les chercheurs et directeurs de projets de développement, des centres de formation et des services de télécommunication, des centres d'études sociétales publics et privés, des gouvernements et des organismes internationaux, comme des opérateurs Internet. Elle est à la disposition des Etats en cas de situations du réseau exceptionnelles.

Les intérêts de la proposition dot-root

technique immédiat ...

Le système de serveurs racine actuellement utilisé pour l'Internet est un système unique sans secours, sans miroir, sans système de test en grandeur réelle, sans système d'évaluation et de contrôle, sans recours en cas de contre-performance, sans statistiques ni autorité technique. Ce

système unique fait l'objet de menaces précises en tant qu'objectif militaire et terroriste. Il est soumis aux tentatives d'intrusion de nombreux pirates. Il a déjà été piraté au moins une fois.

Dot-Root apporte tout d'abord un système de test à l'identique du système opérationnel avec les mêmes machines, les mêmes logiciels, le même plan de nommage réel. Ceci rend possible des tests de versions nouvelles ou d'évaluation de principe (en particulier dans le domaine de la sécurité) que chacun hésite à lancer sur le système de production unique.

le test d'une architecture nouvelle ...

Ensuite, Dot-Root apporte une plate-forme de test de configurations nouvelles, et tout d'abord une architecture parallèle. Ce concept sécuritaire de base semble intuitif, mais il faut le tester, l'optimiser et en découvrir les règles opérationnelles pour un système d'une telle taille, et sans aucun doute tester des alternatives architecturales (en particulier dans la manière d'utiliser et de diffuser ces données).

Si la gestion concertée d'un tel système parallèle de serveurs racine paraît nécessaire à la sécurité de l'Internet, elle doit avoir aussi été pensée, testée et organisée dans un contexte international ouvert – y compris aux pays en développement, ce qui fait Dot-Root qui est une proposition de la Communauté Internet Globale, y compris de pays en voie de développement. C'est un atout technique pratique que n'auraient pas les projets purement nord-américains encore à l'étude. Des gestionnaires de serveurs DNS des cinq continents ont signifié leur intérêt.

l'outil pour la recherche de réponses socialement attendues ...

Le fichier maître utilisé sur le système de production est sous contrôle unique du gouvernement américain. Celui-ci peut donc décider de tout e-embargo et de tout routage alternatif. Ce gouvernement dispose ainsi, par ses archives, d'informations exclusives sur l'utilisation du réseau, et potentiellement sur l'économie et la vie des pays et de leurs utilisateurs, pourtant nécessaires à l'application de leurs lois de sécurité intérieure. Il décide unilatéralement des TLD supportés et complique, au point de les interdire dans la pratique, les développements locaux, commerciaux, culturels tirant parti du nommage qui ne sont pas du choix de ses industriels ou de ses politiques.

Dot-Root en étant une plate-forme pour le développement, le test et le prédéploiement de tout projet de la communauté Internet va permettre de vérifier en vraie grandeur les problèmes s'il existe ou non des problèmes liés au nombre de suffixes, comment organiser des visions locales du réseau (comme le fait par exemple le Viêt-nam) sur une échelle mondiale (et donc permettre le déploiement d'internet de proximité).

et techniquement urgentes ...

Ainsi nombre de questions majeures, aujourd'hui sans réponses observées, qui conduisent à une gestion sur-précautionneuse et à un statu quo favorable aux positions acquises, vont pouvoir être résolues de façon transparente. Ceci concerne des préoccupations telles que : la sécurité, le support du téléphone, les adresses IPv6, les noms de domaines multilingues, les annuaires, les services étendus. Tous réclament un tel outil et font de la proposition dot-root une réponse certainement utile à nombre de besoins réels.

dans le contexte du consensus mondial qui vient d'être réaffirmé ...

Elle se situe également en droite ligne de l'évolution toute récente de la "charte internationale" de l'Internet, tel que vu par les Etats, qu'est la proposition 102 de l'Union Internationale des Télécommunications. D'origine privée très "à la internet", elle apporte un outil d'expérimentation très simple et peu onéreux d'une gestion en concertation internationale entre intérêts privés et droits et devoirs des souverainetés nationales.

une proposition simple et sérieusement pensée ...

Cette proposition est fondée sur une expérience de 25 ans de ce contexte par son promoteur et sur celle, acquise depuis deux ans, de trois opérateurs de root expérimentaux européens. Ils coopèrent depuis plus d'un an et ont déjà une pratique et des outils d'opérations comparables ou communs.

Elle se situe dans la continuité technique de la communauté Internet. Les premiers "drafts" pour l'information de l'IETF son en cours de préparation. Mais elle veillera à garder informées les autres structures internationales concernées : IUT, OMPI, OMC, EDIFACT, etc.

La gestion concertée de sa plate-forme est séparée des projets de développement. Elle ne vise qu'à les héberger, en leur apportant des conditions optimales et les solutions nouvelles qu'ils auront confirmées au fil de leurs résultats, au sein de ces structures internationales.

Le soutien apporté à un moniteur externe complète le dispositif technique pour un compte-rendu tiers, en temps réel, des opérations de ce service. Une formule originale d'espaces de nommage de test (pour le trafic, la charge du grand nombre, pour les aspects sociétaux) permet d'associer aux validations, un public de test nombreux sans déséquilibrer le réseau général.

Tout ceci vise à laisser les chercheurs pleinement libres et à permettre une analyse des projets totalement indépendante, propre à l'éclosion de l'innovation, jusqu'à une implémentation réelle

Un comité de pilotage pour l'orientation de la recherche, et un comité consultatif ouvert à tous les professionnels reconnus des réseaux, devraient conforter cette indépendance et catalyser des projets utiles et innovants, tout en permettant aux gestionnaires des serveurs dot-root de bénéficier de la meilleure assistance pour leur apporter le meilleur support.

Issue d'une réflexion conduite au sein de la DNSO (section de l'ICANN tournée vers le DNS) et en particulier de son assemblée générale (GA) et de son collègue des entreprises (BC), un Institut pour la Sécurité et la Stabilité du Réseau y sera associé.

un facteur de stabilité immédiat ...

La première nécessité pour "dot-root" est celle d'un fichier international des suffixes tenu à jour. Ce fichier fonde les légitimités mutuelles des "co - opérateurs" de l'espace de nommage de l'Internet. Le but est d'expérimenter s'ils peuvent l'administrer en concertation et en automatiser la tenue à jour. Si ce simple projet initial réussit, se stabilise et s'étend aux suffixes actuels, l'Internet aura, dans les faits, changé de nature.

La gouvernance de l'Internet sera devenue "concertance", non plus soumise "dominance". Le mot "concertation", absent de la langue anglaise, aura trouvé sa traduction.

Jamais, peut-être, "autant n'a dépendu d'un aussi petit budget" (*paraphrase de Churchill*).

- un site commun d'administration et de documentation sous <http://dot-root.com>
- un support collégial des projets au sein du consortium "dot-root", entre les gestionnaires bénévoles des serveurs racine. Les projets sont discutés sur la liste générale de dot-root ou sur les listes des espaces de nommage expérimentaux. Ils sont ensuite revus par les membres d'un comité consultatif qui cherche à aider leur cadrage. Ils sont enfin adoptés par le collège des membres après avoir obtenu le support final de ceux d'entre-eux avec lesquels ils coopéreront.
- leurs projets et résultats sont documentés auprès de l'IETF et de l'IUT, ou des organismes ad-hoc (WIPO, WTO, etc..)
- le secrétariat, la gestion des sites et des listes de discussion, l'organisation de rencontres de travail, d'information et de formation mutuelle, la gestion des enregistrements dans les espaces de nommage de test sont assurés par des organisations externes, appointées par le conseil des administrateurs des systèmes racine.
- un comité de pilotage de 12 membres est sélectionné par les membres, les administrateurs et le comité consultatif à raison d'un tiers chacun : son rôle est d'animer la communauté Internet dans son utilisation du système dot-root et l'évolution du DNS.

Objectifs d'ici la fin 2002

- stabilisation du site dot-root en Anglais - listes de diffusion en place
- stabilisation des systèmes d'administration des groupes de serveurs racine
- test du monitoring et discussion des informations qu'ils demandent
- implémentation des systèmes de collecte des données
- implémentation du système de collecte de cotisations pour le Secrétariat
- installation des premiers ULD de test (.univ, .telco)
- addition de serveurs candidats sur Boroon et Cinics
- validation des systèmes initiaux de production et de mise à disposition des fichiers racine

- documentation IETF du système
- sélection du comité de pilotage
- invitations initiales au comité consultatif
- présentations d'informations sur le site – organisation du système d'édition

- mise en place des ULD universitaires et télécom
- collecte de des premiers projets et présentation au comité consultatif
- information des ccTLDs et tests de collecte des données

- recherche de financement sous forme de contribution et de missions/rapports de conseil
- promotion des ULD pour y trouver un financement annexe stable
- mise en place de l'e-zine news@dot-root

- préparation d'une réunion internationale dot-root pour février 2003

Budget

Le projet "dot-root" est un projet Internet qui fait appel aux contributions "en nature" de ses partenaires. Son seul coût est celui du fonctionnement de sa cellule d'animation que constitue son Secrétariat.

Ses ressources sont :

- la commande de rapports personnalisés sur dot-root et l'aide à la proposition de projets
- la collecte des cotisations des Membres des espaces de nommage (activité de registre)

Les autres fonctions centrales se rémunèrent sur l'aide qu'elles apportent. Des contributeurs (entreprises, sponsors) au projet peuvent vouloir prendre certains coûts à leur charge : ce sponsoring est alors documenté sur le site <http://dot-root.com>