

L'Internet, vecteur de puissance des Etats-Unis ?

## **3 - Contrôle politique et technique de l'Internet**

mercredi 13 septembre 2017, par [Laurent BLOCH](#)

**Laurent Bloch aborde dans ce troisième chapitre le contrôle politique et technique de l'Internet. De façon très accessible il présente les institutions de l'Internet et le système de noms de domaines (DNS). Il s'interroge : l'ICANN est-elle un moindre mal ? Peut-on envisager l'exclusion du DNS comme punition ? L. Bloch explique encore le routage dans l'Internet et l'interconnexion de réseaux.**

***Diploweb.com*, publie cet ouvrage de Laurent Bloch, *L'Internet, vecteur de puissance des Etats-Unis ?* pour proposer à chacun les éléments nécessaires à une juste appréciation de la situation. Ce livre est déjà disponible sur Amazon au [format numérique Kindle](#) et [au format broché imprimé sur papier](#). Il sera publié ici sous forme de feuilleton, chapitre par chapitre, au rythme d'environ un tous les trois mois.**

L'Internet est une institution de fait, dotée d'organes de pilotage relativement informels mais qui déterminent (plus ou moins) son fonctionnement et les rapports de force entre les acteurs. Il a beaucoup été question, en cette année 2016, du désengagement des États-Unis à l'égard de l'ICANN (un de ces organes dont nous décrivons ci-dessous le rôle et le fonctionnement), mais, outre que l'ICANN n'est pas le seul véhicule de l'influence américaine sur le réseau, sa réorganisation pourrait ne rendre que plus discrète cette influence, qui repose en dernière analyse sur la supériorité de leur production tant intellectuelle qu'industrielle.



### **Institutions de l'Internet**

Quelles sont les instances de pilotage de l'Internet ?

. L'Internet Architecture Board (IAB) est le comité qui supervise le développement technique et l'ingénierie de l'Internet ([www.iab.org](http://www.iab.org)).

. L'Internet Society (ISOC) est un organisme de discussion qui regroupe 80 organisations et 28 000 adhérents individuels, et qui détient une influence importante dans certains débats ([www.isoc.org](http://www.isoc.org)).

. L'Internet Engineering Task Force (IETF) est un forum technique créé en 1986, supervisé par l'IAB qui élabore et valide les normes techniques de l'Internet. L'IETF fonctionne sur la base du volontariat, les industriels du secteur des réseaux y délèguent des ingénieurs pour consolider leur influence et faire prévaloir leurs choix techniques. Entre 1000 et 2000 personnes assistent aux réunions plénières, mais l'essentiel du travail est accompli via le réseau ([www.ietf.org](http://www.ietf.org)). L'IETF assure la rédaction et la diffusion des Requests for Comments (RFC), qui sont les documents de normalisation du fonctionnement de l'Internet.

. L'augmentation du volume d'activité de l'IETF a conduit à la création de l'Internet Engineering Steering Group (IESG), chargé d'en coordonner l'activité.

. L'Internet Corporation for Assigned Names and Numbers (ICANN) est une organisation à but non lucratif, créée en 1998 pour prendre en charge un certain nombre de tâches de gestion de l'Internet, notamment les missions stratégiques que sont la réglementation et l'attribution des adresses et des noms ([www.icann.org](http://www.icann.org)). L'ICANN est formellement sous le contrôle du Department of Commerce américain, ce qui a été confirmé officiellement en juillet 2008.

. Une mention particulière doit être réservée à l'Internet Assigned Numbers Authority (IANA), qui est depuis 1998 une fonction confiée à l'ICANN pour centraliser et contrôler les conventions relatives à l'identification des objets du réseau et notamment pour veiller à l'unicité des adresses, mais qui à sa création en 1988 était une organisation autonome.

## **Le système de noms de domaines (DNS)**

Si aujourd'hui depuis un cybercafé de Macao vous pouvez consulter le solde de votre compte sur le site de votre banque française, ainsi que l'état de votre commande chez Amazon en Virginie, c'est grâce à l'Internet, bien sûr, mais si vous pouvez le faire *facilement* c'est grâce au système de noms de domaines, le DNS. Fonctionnellement, c'est un simple annuaire : dans la colonne de gauche les numéros IP (analogues aux numéros de téléphone), dans la colonne de droite les noms des domaines correspondants, comme par exemple <http://www.diploweb.com>. Techniquement, c'est un des rouages les plus merveilleux de l'Internet, une base de données distribuée mondiale, mise à jour automatiquement par les abonnés eux-mêmes et en temps (presque) réel, dont la racine, organisée logiquement autour de 13 serveurs, est répartie physiquement sur des centaines de machines de par le monde [1] (de même, il existe une carte des points d'échange de l'Internet (IXP) [2] et une carte des fibres optiques transocéaniques [3], indispensables à la compréhension du cyberspace ; cf. aussi cet article sur les câbles sous-marins [4]). Cela marche si bien parce que ce système est unique, et univoque : des centaines de bureaux d'enregistrement coopèrent de par le monde afin que de Macao vous puissiez apprendre le numéro IP de la Banque agricole de Paizay-le-Tort dans les Deux-Sèvres, sans même avoir à vous en occuper, votre navigateur Web le fait pour vous. À un nom de domaine correspond un serveur unique (éventuellement répliqué sur plusieurs machines physiques et sur plusieurs sites), sans ambiguïté.

---

## Unicité menacée du DNS

L'unicité du système de noms de domaines est remise en cause de plusieurs façons. La démarche la plus sérieuse dans cette direction est la création par [la Chine](#) de sa propre racine du DNS, qui pour l'internaute chinois se substitue entièrement au DNS mondial, ce qui a pour effet de lui rendre inaccessibles les sites étrangers. Ainsi, s'il tapait (avant le retrait de Google en 2010) [google.com](http://google.com), il accédait (et il pourra sans doute bientôt à nouveau accéder) en fait à [google.com.cn](http://google.com.cn), version sinisée et dûment expurgée du site. Les Chinois ont profité de ce bouleversement pour déployer la version 6 du protocole de réseau IP [5] en lieu et place de la version 4, et pour généraliser l'emploi des idéogrammes dans les adresses Web et de courrier électronique. Il a fallu pour réaliser ces transformations mobiliser des milliers d'ingénieurs, des centaines de millions de yuans et des années de travail. Il faut pour expurger l'Internet mondial des dizaines de milliers d'employés de la censure, en plus des logiciens qui dégrossissent le travail. La justification officielle de cette opération est de permettre à l'internaute chinois de naviguer sur le Web en utilisant des adresses de sites rédigées dans son écriture habituelle, en idéogrammes, ce qui est bien sûr louable.

Il n'est pas impossible que la prouesse chinoise ne lui attire des imitateurs, ou des clients, du côté de certains régimes politiques qui ne souhaitent pas vraiment que leurs sujets aient un accès trop libre à une information mondiale.

Si ce genre de pratique se répand, le risque est la balkanisation de l'Internet : on serait ramené des décennies en arrière, à ce qu'était l'usage du réseau avant l'Internet, avec Transpac, les réseaux X25 et la messagerie X400.

Il ne faut pas pour autant négliger les aspects positifs de l'expérience chinoise : elle démontre que le DNS peut fonctionner avec un système de nommage qui repose sur une écriture différente de l'alphabet latin, et que la mise en place d'une racine alternative n'est pas trop difficile. Et aussi, qu'il n'y a aucune raison ontologique de faire allégeance à l'ICANN (Internet Corporation for Assigned Names and Numbers), l'organisme qui supervise le DNS mondial, sous le contrôle du gouvernement américain.

## L'ICANN est-elle un moindre mal ?

Face à ce qu'il faut bien appeler les abus de pouvoir de l'ICANN et à la mainmise américaine sur l'Internet, dont les révélations d'Edward Snowden (notamment au sujet de l'affaire PRISM) nous ont confirmé qu'elle n'était pas uniquement inspirée par un souci technique bienveillant, on peut se poser la question d'une gouvernance différente : sous le contrôle de l'ONU ? par l'UIT (Union internationale des télécommunications, une agence de l'ONU) ?

L'UIT est un organisme du passé, complètement extérieur à la vie de l'Internet. Veut-on le retour à la bureaucratie des opérateurs en situation de monopole ?

Quant à l'ONU, veut-on vraiment qu'aient voix au chapitre des gouvernements qui souhaiteraient que sur l'Internet il soit interdit de dire du mal des autorités religieuses, ou des gouvernements ?

Bref, il faut sans doute chercher ailleurs.

## L'exclusion du DNS comme punition

D'autres tractations menacent le fonctionnement du DNS, et par voie de conséquence celui de l'Internet : les législateurs de plusieurs pays occidentaux, au nombre desquels la France et les États-Unis, ont pensé que pour faire appliquer des lois telles que Hadopi ou la Loppsi pour la France, ou le *Digital Millenium Copyright Act* (DMCA) et ACTA pour [les États-Unis](#), la meilleure façon serait de rayer du DNS les sites contrevenants, par réquisition de justice auprès des opérateurs. L'affaire Megaupload [6] a montré que cette forme d'administration de la justice pouvait prendre une extension internationale. On peut même imaginer punir des pays entiers, en créant à la place de leur zone du DNS (par exemple la zone .fr pour la France) un « trou noir ».

C'est possible pour un état très influent comme les États-Unis, qui contrôle l'ICANN et qui a les moyens de convaincre la justice néo-zélandaise de se rallier à ses démarches ; des pays moins hégémoniques obtiendront des résultats moins spectaculaires, mais de toutes les façons c'est une très mauvaise idée, comme nous allons tenter de le montrer.

Tout d'abord, cette mesure est en effet d'une efficacité limitée. Priver un site d'enregistrement dans le DNS ne suffit pas à en bloquer l'accès. De même que si vous voulez téléphoner à un ami qui est sur liste rouge, vous le pouvez dès lors que vous connaissez son numéro, vous pourrez toujours atteindre les sites proscrits si vous connaissez leurs numéros IP. C'est d'ailleurs ainsi que fonctionnent les réseaux pair à pair, qui ont représenté jusqu'à 80 % du trafic de l'Internet avant d'être supplantés par des sites tels que Megaupload, et qui reprennent leur essor, avec des techniques plus puissantes, depuis la fermeture de ce site. Le DNS est très utile et très commode, mais on peut s'en passer.

Il est également possible de créer une racine alternative : outre celle des Chinois, il existe quelques projets dans ce domaine, notamment OpenDNS, sans grand retentissement jusqu'à ce jour, mais qui pourraient connaître le succès s'il s'avérait que la racine du DNS de l'ICANN était vouée à une évolution brejnévienne [7].

L'Internet pourrait donc fonctionner sans le DNS : simplement, il y perdrait la facilité d'usage, l'ubiquité et l'uniformité de méthode d'accès qui font son universalité. Au lieu de taper sans avoir à réfléchir l'adresse de votre banque poitevine, que vous soyez à Macao ou à Puntas Arenas, vous auriez à vous renseigner : quel est le meilleur DNS disponible en Patagonie ? un accès pair à pair est-il possible depuis votre hôtel au Tadjikistan ? Il faudrait configurer votre smartphone en conséquence. Inutile de dire que si les informaticiens de métier devraient réussir à s'en débrouiller, les personnes qui avaient déjà eu du mal à apprendre l'usage du courrier électronique et du Web passeraient par des moments difficiles ou abandonneraient. Bref, ce merveilleux moyen de communication serait cassé.

Certaines voix s'élèvent pour revendiquer l'introduction d'un peu d'ambiguïté dans le DNS : un même nom de domaine pourrait désigner plusieurs services, qui seraient proposés à l'internaute, qui choisirait. J'avoue ne pas très bien comprendre l'intérêt de cette démarche : l'existence d'homonymes dans le monde des humains est une situation de fait, qui a quelques inconvénients et aucun avantage, si on peut s'en passer dans l'espace de noms artificiel du DNS, cela n'a que des avantages, et l'introduire n'aurait que des inconvénients, juste agaçants pour les humains, rédhibitoires pour les programmes.

## Le routage dans l'Internet

Rappelons-nous ceci : chaque ordinateur connecté à l'Internet (ou « nœud » du réseau) est doté d'une adresse IP, ou numéro IP, qui, comme le numéro de téléphone dans le réseau téléphonique, est unique et permet de l'atteindre depuis n'importe quel autre nœud du réseau, n'importe où dans le monde.

Les internautes qui veulent visiter un site n'en connaissent généralement pas l'adresse IP, mais le nom, comme par exemple [www.diploweb.com](http://www.diploweb.com). L'adresse leur est fournie (ou plutôt est fournie à leur navigateur) par le DNS (Domain Name System), qui est l'annuaire de l'Internet ; comme celui du

téléphone il fait correspondre un numéro IP à un nom. Cet annuaire est réparti sur des milliers d'ordinateurs de par le monde et il est bien sûr mis à jour de façon permanente.

Pour faire circuler des données entre deux nœuds de l'Internet, il faut calculer un itinéraire (en anglais route) entre eux, ce calcul est appelé routage ; si ces nœuds ne sont pas situés sur le même réseau local, l'itinéraire passera par d'autres nœuds, constitués d'ordinateurs spécialisés appelés routeurs. Un routeur est un ordinateur connecté à deux ou plusieurs réseaux, il possède donc plusieurs adresses IP, comme la maison de Balzac qui avait une porte de derrière sur une autre rue, et il est capable de faire passer des données d'un réseau à un autre, en fonction de règles inscrites dans ses tables de routage. Un algorithme de routage calcule des tables de routage.

Actuellement le routage est effectué sur la base des adresses IP fournies par le DNS, mais ce n'est pas une loi de la nature. On pourrait imaginer de tout autres solutions, et d'ailleurs elles existent, telles les systèmes pair à pair évoqués ci-dessus, qui consistent à ce que les participants au réseau s'échangent des tables d'adresses de voisins qui pourront acheminer leurs communications. Cela semble rudimentaire, mais certains experts ont mis au point des systèmes très astucieux et qui fonctionnent très bien, comme par exemple BitTorrent, très utilisé pour la distribution de logiciels en ligne. Et l'on peut imaginer des systèmes d'adressage par le contenu, d'ailleurs Google, Facebook et LinkedIn sont là pour suppléer l'absence d'un tel système (et l'insuffisance du DNS) en nous permettant de retrouver une information par une partie de sa teneur.

## Interconnexion de réseaux

L'Internet n'est pas un réseau unique, mais, comme son nom l'indique, un réseau de réseaux. Chacun de ces réseaux est la propriété d'un opérateur (ou FAI, pour Fournisseur d'accès à l'Internet, en anglais ISP, pour *Internet Service Provider*) différent, qui l'administre à sa façon. Un réseau administré de façon unique par un FAI est un AS (*Autonomous System*) ; si l'on compare l'Internet à un continent, les AS en sont les pays, séparés par des frontières, avec chacun sa législation. Un grand FAI peut posséder plusieurs AS, à l'instar d'un état fédéral. Chaque AS est identifié par un numéro d'AS. L'Internet est constitué de plus de 50 000 AS dont les plus importants comptent des dizaines de millions d'adresses IP.

À l'intérieur d'un AS les routeurs appartiennent au FAI ou à ses clients et sont administrés selon les règles qu'il a fixées. Pour que l'Internet existe et puisse fonctionner, il faut établir des communications entre AS de FAI différents : pour ce « passage de frontière », un FAI disposera des routeurs de frontière de système autonome, directement reliés aux routeurs de frontière des FAI avec qui il veut établir une liaison. Le point auquel seront placés ces routeurs s'appelle généralement un *Internet Exchange Point* [8] (IXP), ou parfois un NIX (Neutral Internet Exchange) ou un GIX (Global Internet Exchange) [9].

Si le trafic entre deux réseaux doit traverser celui d'un FAI tiers intermédiaire, les règles de passage sont fixées par des accords de transit ou d'appairage (peering) entre les FAI, et sont formulées techniquement dans les tables des routeurs selon la syntaxe édictée par le protocole *Boundary Gateway Protocol* (Protocole de passerelle frontalière, BGP). Les accords de transit sont des contrats de service, le réseau émetteur verse des redevances au réseau de transit pour qu'il achemine son trafic. Les accords d'appairage sont par contre généralement basés sur la réciprocité et postulent un certain équilibre, ils ne donnent pas lieu à facturation tant que l'équilibre est respecté, mais il y a des indemnités versées dès que la symétrie des échanges est trop fortement perturbée. On comprend que de tels accords, qui sont le plus souvent ultra-secrets, ne sont possibles qu'entre FAI de tailles comparables, des pairs (peers).

Nous verrons plus loin que ces questions de routage, de transit et d'appairage, très techniques en première approche, ont des aspects politiques et stratégiques qui sont au cœur des conflits à venir dans le cyberspace.

---

## Plus, tout de suite

Ce livre de Laurent Bloch, *L'Internet, vecteur de puissance des Etats-Unis ?*, est déjà disponible sur Amazon au [format numérique Kindle](#) et [au format broché imprimé sur papier](#). Il sera publié ici sous forme de feuilleton, chapitre par chapitre, au rythme d'environ par semestre.

---

## P.-S.

Précédemment responsable de l'informatique scientifique de l'Institut Pasteur, Directeur du Système d'Information de l'Université Paris-Dauphine. Il est auteur de plusieurs ouvrages sur les systèmes d'information et leur sécurité. Il se consacre à la recherche en cyberstratégie. Auteur de « Internet, vecteur de puissance des Etats-Unis », éd. Diploweb 2017.

---

## Notes

[1] <http://www.root-servers.org/>

[2] <http://internetexchangemap.com/>

[3] <http://www.submarinecablemap.com/>

[4] <http://fr.wikipedia.org/wiki/C%C3%A...>

[5] La version 6 du protocole IP répond à la pénurie imminente de numéros IP par un changement de système de numérotation, exactement pour les mêmes raisons qu'en France nous sommes passés des numéros de téléphone à six ou sept chiffres aux numéros actuels à dix chiffres. La norme actuelle (IPv4) repose sur des numéros à 32 chiffres binaires, ce qui autorise un maximum théorique de quelques quatre milliards de numéros (4 294 967 296 précisément), mais en pratique moins, parce que, comme pour les numéros de téléphone, la structure des numéros fait que certains intervalles ne sont pas utilisés. Les numéros IPv6 ont 128 chiffres binaires, ce qui autorise théoriquement quelques  $3,4 \times 10^{38}$  adresses.

[6] Megaupload était un site de téléchargement créé par un citoyen allemand surnommé Kim Dotcom, et qui proposait en ligne des fichiers sans trop se préoccuper des droits d'auteur qui pouvaient les protéger. La justice américaine a ordonné la fermeture du site, la radiation de son nom de domaine du DNS, et obtenu des autorités de Nouvelle-Zélande l'extradition de Kim Dotcom, qui résidait dans ce pays.

[7] Pour les lecteurs les plus jeunes qui n'auraient pas connu le monde d'avant la chute du mur : Léonid Brejnev fut un des derniers dirigeants de l'URSS, acharné dans la répression de toute pensée libre et indépendante, totalement fermé à toute idée d'évolution, aussi rigide que le permafrost, le sol gelé de la Sibérie.

[8] <http://fr.wikipedia.org/wiki/Intern...>

[9] Les principaux IXP sur le sol français sont *France Internet Exchange* (France IX), Paris, *Lyon Internet Exchange*, administré par l'association Rézopole, *Equinix Exchange Paris*, *Service for French Internet Exchange* (SFINX), administré par RENATER, entre Paris et Aubervilliers.