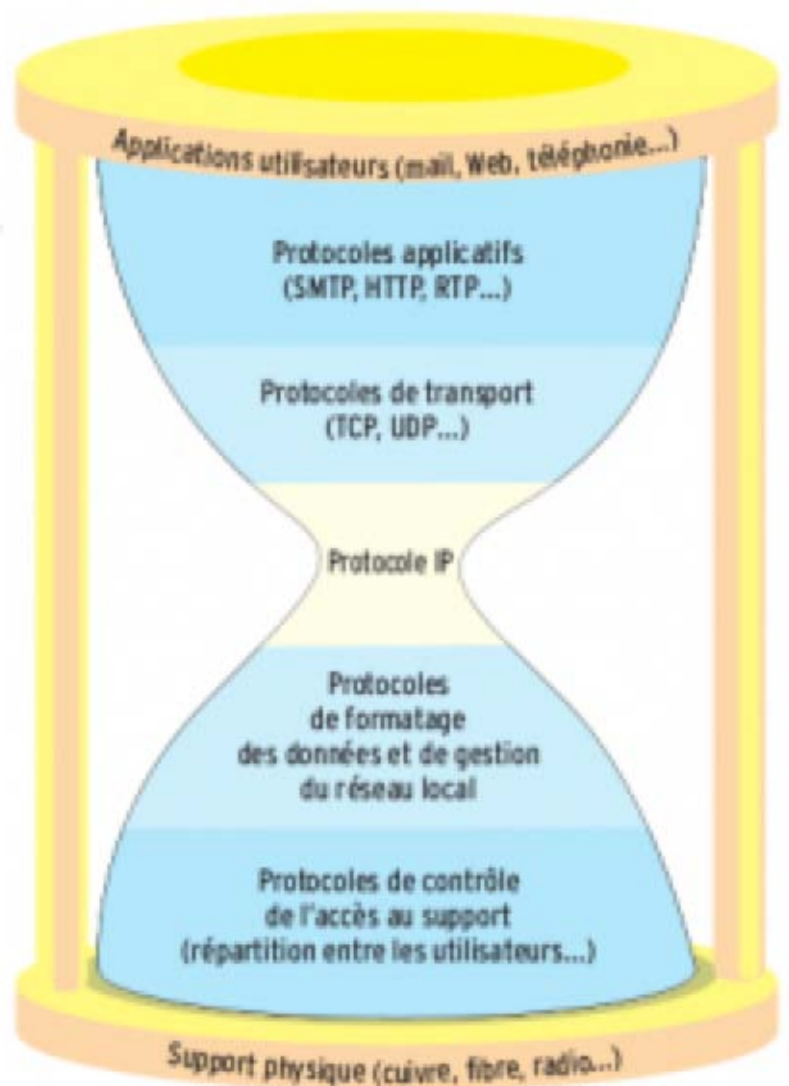


Le routage, enjeu de cyberstratégie



Kavé Salamatian, octobre 2012,

que l'Internet est un espace stratégique dont l'importance dépasse les seuls enjeux techniques et technologiques. Il devient donc crucial de comprendre son architecture et la compréhension du routage est fondamentale pour cela.



La sablier IP, représentation des 5 couches de l'Internet

Entretien avec Kavé Salamatian, octobre 2012.

Le Professeur Kavé Salamatian nous introduit à mille lieux sous les liens hypertextes, dans un monde invisible où de grands acteurs se disputent le contrôle des réseaux.

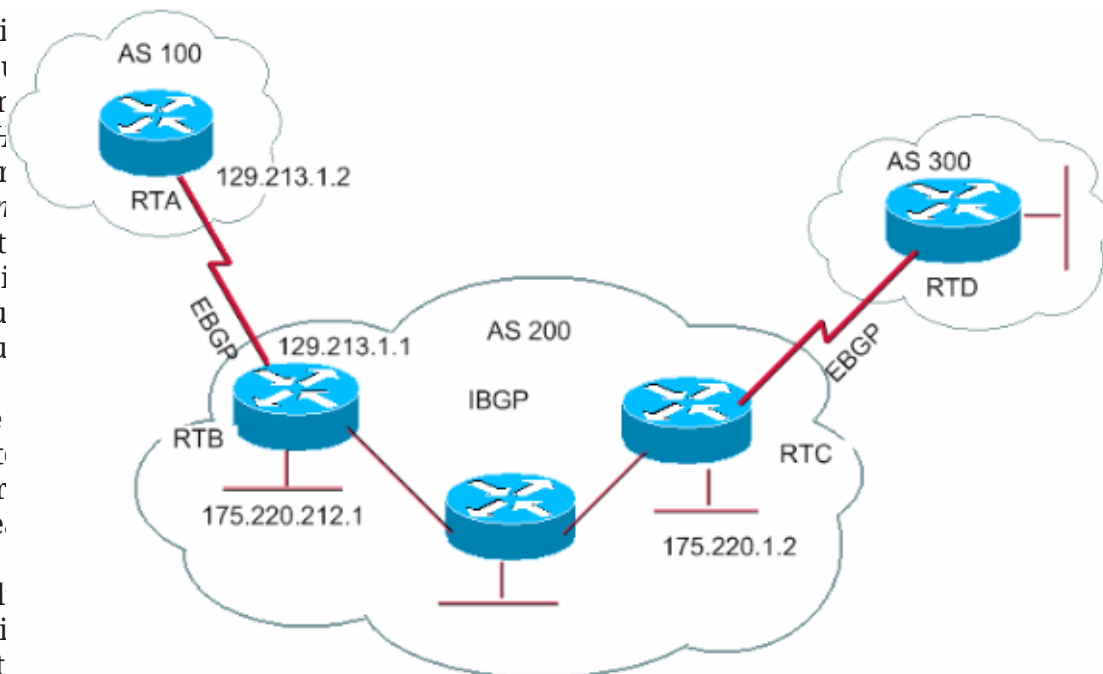
DL : Le routage était il y a peu un sujet réservé des *geeks* spécialisés. Aujourd'hui, il est devenu un sujet de discussion public, évoqué dans des conférences, dans la presse, dans des débats politiques publics d'Internet. Que se passe-t-il ?

Kavé Salamatian : Ce phénomène est dû à la croissance d'Internet. L'Internet est, comme son nom l'indique, un réseau de réseaux. Si l'on compare l'Internet à un continent, il serait peuplé de nombreux systèmes, les AS, qui en seraient les séparés par des frontières, avec chacun sa localisation, sa politique de routage. Il apparaît aujourd'hui

http://reseaux.blog.lemonde.fr/2012/11/04/routage-enjeu-cyberstrategie/

Le routage, enjeu de cyberstratégie

L'Internet est construit sur des protocoles que nous sommes habitués à la voir fonctionner pour des applications. Par exemple, le protocole HTTP (utilisé pour transporter les pages web), le protocole DNS (Domain Name System) pour la résolution de domaines, le protocole SMTP (Simple Mail Transfer Protocol) pour la messagerie électronique, le protocole FTP (File Transfer Protocol) pour le transfert de fichiers, etc. Mais il y a des protocoles de base qui sont le service réseau que nous utilisons tous. Le routage est un service qui s'exécute en permanence. Le rôle du routage est d'assurer une connectivité entre les différents réseaux et les utilisateurs.



Routage BGP, BGP Case studies, Cisco

Sur le plan physique, il y a environ 42 000 AS, chacun avec une adresse IP sur 32 bits. Un AS est un ensemble de routeurs gérés par une seule autorité administrative qui décide des politiques de routage à appliquer. Le plus grand AS est l'AS4134, qui appartient à ChinaNet-Backbone et qui contient 114 164 704 adresses IPv4, suivi de l'AS721 appartenant au Département de la Défense des USA en comportant 89 384 192. Il existe de nombreux petits AS ne contenant parfois qu'un seul ordinateur, par exemple l'AS2111 qui appartient à SkyNet, un fournisseur d'accès établi en Bulgarie.

L'étude du routage consiste à analyser la topologie des AS, c'est à dire la structure de connectivités des AS, leurs relations et leurs dynamiques.

Pour s'échanger des paquets, les AS utilisent des machines spécialisées, des routeurs, qui font circuler l'information dans le réseau en utilisant le protocole BGP, *Border Gateway Protocol*, signifiant en français protocole de passerelle ou de frontière. Les règles de ce protocole permettent à chaque routeur d'annoncer à ses voisins s'ils peuvent accéder à une adresse IP en passant l'AS à laquelle il est rattaché. BGP est le gluant de l'Internet. Ses qualités et défauts, ainsi que la façon dont on l'utilise, conditionnent le bon ou le mauvais fonctionnement des réseaux. Quand j'ai commencé mes études d'informatique, il y avait quelques centaines de personnes connaissant le terme BGP. Depuis quelques années les concepts de BGP sont enseignés dans les formations de réseaux avancées.

Aujourd'hui, l'Internet connaît deux problèmes politiques majeurs au niveau mondial : la sécurité et les modèles économiques des échanges entre les acteurs. Quand on analyse le fond des choses, on tombe forcément sur le fonctionnement du routage.

Le routage, enjeu de cyberstratégie

De plus, les États ont besoin de définir leurs cyberstratégies. Or, mis à part les États-Unis, la Chine et une poignée de petit pays, les autres États commencent tout juste à appréhender les informations et les raisonnements nécessaires pour comprendre ce qui se passe dans les couches basses.

L'Internet est un réseau virtuel bâti sur du réel. C'est un nuage qui prend solidement ses assises dans du béton. Par ses fibres optiques, par ses satellites, par l'environnement politique, légal et économique, l'Internet présente des contraintes physiques, géographiques, économiques, politiques qui ont nécessité des investissements colossaux. La géographie de l'Internet, ce qu'on appelle la cyber-géographie est un enjeu majeur de la cyber-stratégie.

DL : Dans les enceintes multilatérales, quand on parle des ressources critiques, on évoque surtout le DNS, pour dénoncer son contrôle par le Département du Commerce des États-Unis.

KS : La question du nommage n'est pas stratégique. Mais ce serait une erreur stratégique de ne pas s'en préoccuper. Néanmoins c'est moins important que le routage. À quoi servirait d'avoir un nommage quand on n'a pas de connectivité ?

Internet est fondé sur un ensemble de règles, les protocoles. Le protocole IP (*Internet Protocol*) définit pour chaque interface réseau une adresse IP unique sous forme de quatre nombres séparés par des points dans la version du protocole, appelée IPv4. Par exemple, 194.2.0.30 est une adresse IP correspondant à *elysee.fr*. Ce système, codé sur 32 bits, permet au maximum l'attribution d'un peu plus de 4 milliards d'adresses, plus précisément 2 élevé à la puissance 32. En pratique de par la structuration de l'espace IP en classes d'adressage, il y a beaucoup moins d'adresses disponibles.

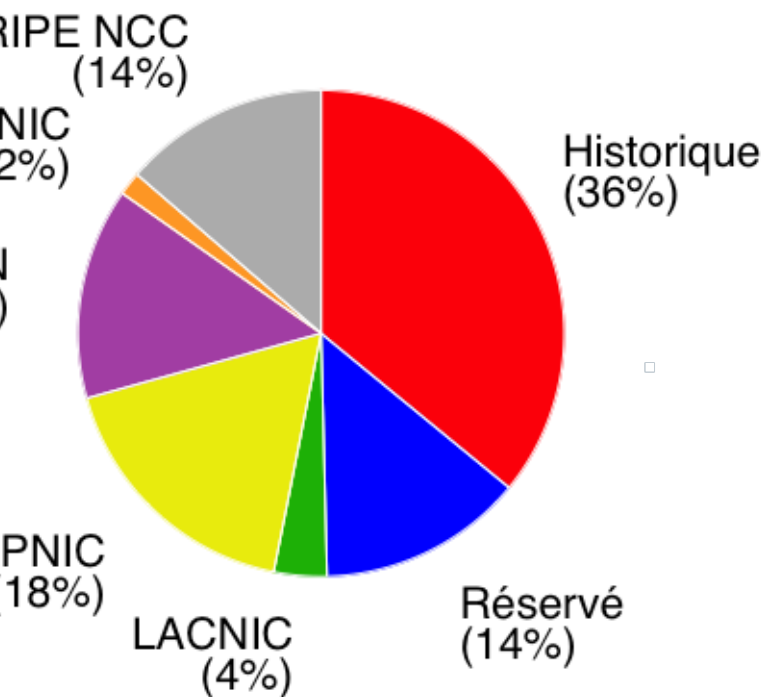
Jusqu'au début des années 1980, l'Internet ne traitait que des adresses IP sous forme de séries de nombres. Au milieu des années 1980, on a ajouté à l'architecture de l'Internet un service applicatif per-

mettant de manipuler aussi des noms de domaines en lettres, plus faciles à lire pour des humains et correspondant aux adresses IP, réservées aux machines. C'est ce mécanisme de mise en relation d'un nom canonique à son adresse IP en chiffres qu'on appelle DNS. Ce mécanisme ne fait pas partie intégrante de l'architecture de l'Internet. Ce n'est qu'une application.

Si on supprimait le nommage aujourd'hui, l'architecture de l'Internet n'en serait pas modifiée pour autant. D'ailleurs on constate que l'utilisation du nommage diminue. Nombre d'utilisateurs n'écrivent jamais une URL dans la barre d'adresses. Ils écrivent dans la zone de recherche et cliquent ensuite sur les liens proposés. Des univers entiers, comme Facebook, échappent au DNS. Google pourrait très bien court-circuiter le nommage s'il y voyait un intérêt. L'aspect nommage est donc séparé de l'aspect routage. Le nommage en lui-même est moins important que la garantie de connectivité.

DL : Comment expliquez-vous la lenteur du passage à IPv6 alors que les adresses IPv4 sont épuisées ?

Le routage, enjeu de cyberstratégie



Distribution des blocs IPv4, CC Mro, Wikipedia

pénurie d'adresses, tandis qu'introduire IPv6 demande d'investir et de re-réfléchir l'architecture de son réseau, ce à quoi le tissu industriel est très réticent. Mais il y a trois exceptions où le déploiement d'IPv6 est une nécessité :

1- Quand on a besoin de beaucoup d'adresses routables, comme pour l'Internet mobile. Par exemple le trafic mobile de la Corée du Sud est supérieur à celui des États-Unis dans leur ensemble.

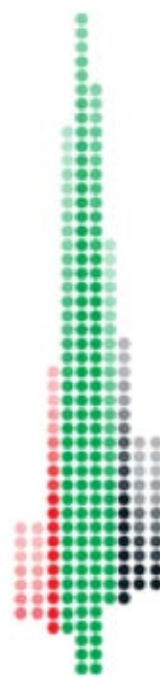
2- Pour les nouveaux entrants, comme la Chine, c'est une occasion de rectifier un déséquilibre fondamental dans la répartition des adresses. La distribution d'IPv4 résulte d'un historique de 40 ans d'Internet...

3- Lorsqu'on veut construire un îlot d'Internet consistant, connectable mais facilement séparable. En Iran, c'est un projet depuis longtemps. Ce qui montre bien le rapport entre interconnexion et stratégie.

KS : En effet, l'expansion d'Internet a fait que le stock d'adresses IP a déjà été épuisé en février 2012. On commence même à assister à des ventes d'adresses IPv4 alors qu'elles ne peuvent en théorie pas être commercialisées, contrairement au DNS, vite transformé en service commercial. Fin 2011, le libraire américain Borders, a fait faillite. Il détenait un portefeuille de 65 536 adresses IPv4. Elles ont été liquidées à 12 \$ l'adresse.

IPv6 a été mis au point, il y a environ 15 ans, en prévision de la pénurie d'adresses IPv4 et pour faire face à des besoins d'identifiants largement supérieurs. Les adresses IPv6 sont codées sur 128 bits. Cela fait un nombre d'adresses qui s'écrit 34 suivi de 37 zéros, c'est-à-dire un nombre difficile même à nommer.

Bien que nous n'ayons plus d'adresses IPv4 à distribuer, IPv4 ne disparaîtra pas à moyen terme. En effet, IPv6 n'est pas adopté rapidement parce qu'il n'offre rien de nouveau qu'on ne puisse pas faire avec IPv4. Il existe des artifices pour faire face à la



WCIT2012
World Conference on International
Telecommunications
Dubai, UAE

En décembre 2012, à Dubaï, une Conférence mondiale des télécommunications internationales (CMIT-12, en anglais WCIT-12) doit mettre à jour le Traité qui date de 1988, les fameux ITRs, *International Telecommunications Regulations*.

Ce traité a plus de 30 ans. Depuis, des changements majeurs ont

http://reseaux.blog.lemonde.fr/2012/11/04/routage-enjeu-cyberstrategie/

Le routage, enjeu de cyberstratégie

transformé le paysage des télécommunications dans le monde entier : privatisations, dérégulation, création de régulateurs nationaux, expansion d'Internet.

Un projet de traité révisé a été soumis à discussion par l'Union Internationale des télécoms, l'agence spécialisée de l'ONU. Le débat fait rage en ce moment. Depuis des mois, les grands acteurs américains dénoncent une présumée tentative de prise de contrôle de l'Internet.

DL : Dans le projet de nouveau Traité international des télécoms, rien ne semble mettre en cause les attributions de l'Icann et de son écosystème en matière de gouvernance Internet. Pourquoi assiste-t-on à un tir de barrage des organisations américaines, Vinton Cerf en tête ? Pourtant, en 1992, l'Isoc, l'*Internet Society*, préconisait que l'Internet soit géré par l'UIT. L'Isoc était alors présidée par Vinton Cerf qui l'avait cofondée pour servir de support aux travaux de standardisation de l'IETF (*Internet Engineering Task Force*).

KS : L'UIT et l'IETF ont beaucoup divergé. Elles ont des profils très différents. L'une a 150 ans d'existence et a longtemps rassemblé des représentants des États. L'autre est issue de la culture libertaire des campus américains des années 70. Même les codes vestimentaires sont opposés. À l'UIT, on porte des costumes Armani, on parle un langage diplomatique. À l'IETF, on voit des tenues très diverses mais beaucoup de *tee shirts*, casquettes et des chaussettes de laine qui montent jusqu'au cou. Et on trinque avec des chopes de bière. Les deux milieux se tiennent en mépris réciproque.

Avec la libéralisation, l'UIT est devenue un club qui a pour ligne de mire les bénéficiaires des opérateurs. On n'attend pas du Medef qu'il pousse le droit du travail dans l'intérêt des employés. Il ne faut pas attendre de l'UIT qu'elle défende les intérêts des internautes. L'UIT établit des accords entre opérateurs, par consensus, pour faire quelque chose. Elle

normalise des fonctionnalités. L'IETF est construite sur une autre conception. Elle réunit des groupes d'experts pour résoudre des problèmes, élaborer des solutions. Elle standardise des interfaces.

Néanmoins toutes ces organisations coopèrent. Elles y sont obligées et le devront de plus en plus. Pour se rapprocher, c'est assez simple. Il faudrait déjà se respecter. À ma connaissance, l'UIT n'a commencé que depuis peu des contacts académiques et je ne l'ai pas vue recruter des personnes ayant été responsables de groupes de travail à l'IETF. À l'IETF, il n'y a pas de salariés ou de recrutement, et à ma connaissance, cela n'intéresse pas les gens de l'UIT de travailler bénévolement.

Pour Dubaï, si l'UIT était définie comme seul cadre international pour gérer les télécoms, cela ne marcherait pas. Elle n'a plus les compétences techniques. Et un consensus vague, cela équivaudrait à rien.



Site Internet de la BBC en persan, 2012, bloqué en Iran

Prenons un exemple. Depuis quelques temps, l'accès à la BBC, diffusée gratuitement par satellite en Europe, est bloqué. En Iran, les sites Internet de la BBC sont filtrés depuis longtemps. Mais la chaîne BBC en persan est très écoutée dans le monde, par les Iraniens d'Iran et par l'importante diaspora. Les autorités iraniennes parasitent les émissions.

http://reseaux.blog.lemonde.fr/2012/11/04/routage-enjeu-cyberstrategie/

Le routage, enjeu de cyberstratégie

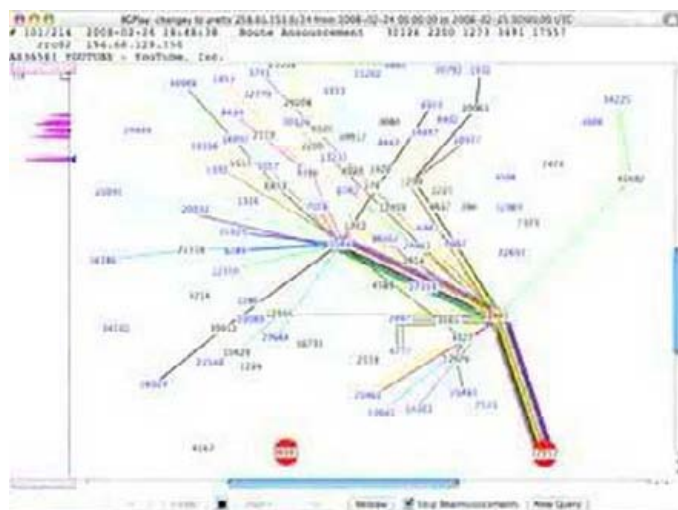
Même les informations en anglais ne passent plus à Londres. L'UIT est mandataire pour ces questions. Elle devrait régler ça, soit en saisissant la Cour internationale de justice à La Haye, soit en envoyant une injonction à Intelsat. Finalement après 5 années d'interférences, l'accès des chaînes de télévision iraniennes aux satellites a été récemment réduit. Mais l'argument n'a pas été celui de la violation de règles internationales, seulement celui des sanctions internationales.

DL : Pensez-vous qu'il faille réguler l'interconnexion des réseaux ?

KS : L'interconnexion entre domaines, c'est la zone grise de l'internet.

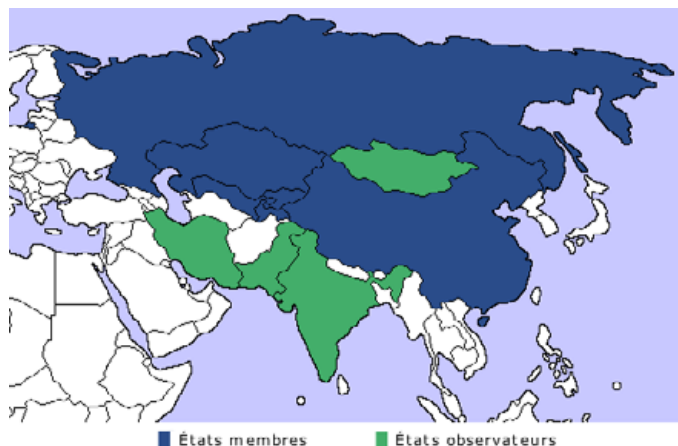
Le routage, c'est le paradis d'Adam Smith. C'est un monde opaque, avec une prédominance d'acteurs privés et internationaux. Le marché y est roi. Donc on y rencontre tous les problèmes des marchés non régulés : abus de position dominante, ententes etc. Une régulation mondiale pourrait poser les cadres d'une connectivité minimale. Elle pourrait s'inspirer par exemple de l'accord postal de 1870. Elle pourrait réduire la fracture d'interconnexion et éviter le syndrome de la mobylette pakistanaise : c'est un cas d'anthologie de coupure par fausse annonce BGP qui se retourne contre l'agresseur. Elle est immortalisée par une vidéo (voir ci-dessous, NDLR) où l'on peut suivre toutes les étapes de routage avant, pendant et après l'incident. Le gouvernement pakistanais a voulu couper YouTube suite à la publication d'une vidéo jugée blasphématoire. Il a ordonné à Pakistan Telecom de couper l'accès à YouTube. Pour y parvenir, l'opérateur a utilisé une possibilité de BGP qui est d'émettre une fausse annonce, du genre « *Pour YouTube, venez par ici, c'est le plus court chemin.* » Ils ont détourné le trafic de YouTube vers eux. YouTube a en effet été coupé pendant 5 minutes dans le monde entier et pendant quelques heures dans certaines parties du monde, le temps que ses gestionnaires reprennent la situation en mains. C'est ce qu'on appelle un *BGP hijack*. Mais les télécoms du Pakistan, submergées par l'importance des flux qui étaient destinés à YouTube, ont été mises hors

service. On ne pouvait même plus téléphoner pour avertir les responsables. Il a fallu envoyer un courrier en mobylette.



Pour les problèmes de *BGP hijack* et autres attaques informatiques, il faudrait pouvoir recourir à un tribunal arbitral.

DL : Les États-Unis ne veulent pas de traité international sur ce sujet. L'Organisation de coopération de Shanghai a conclu un accord de cybersécurité entre ses pays membres. Comment convaincre les États-Unis de s'en remettre à une régulation internationale ?



Organisation de coopération de Shanghai, 2012

Le routage, enjeu de cyberstratégie

KS : L'Organisation de Shanghai, c'est comme une association d'alcooliques anonymes qui œuvrerait pour interdire la vente d'alcool. Il est à noter que les États-Unis alimentent cela de façon détournée en prenant des postures morales au sujet de l'Internet. Mais pour avoir une position morale, il faut un minimum de moralité. Ils se livrent à de la prédication avec un pistolet à la ceinture. Stuxnet et Flame sont des arguments donnés aux régimes autoritaires pour fermer leurs réseaux en arguant de motifs de sécurité.

Les États-Unis refusent totalement d'entrer dans un quelconque cadre de régulation internationale de l'Internet. Ils accepteront de contribuer à chercher une solution quand le pragmatisme les y mènera.

DL : Quand ils verront le morcellement d'Internet tant redouté ?

Il y a des signes de morcellement, en effet. La Chine, l'Iran et d'autres. Par exemple, le Japon est quasiment en Intranet, mais ce n'est pas le résultat d'un plan délibéré : cela résulte de traits culturels et linguistiques. Les échanges des Japonais se font essentiellement entre eux.

Il y aura morcellement visible quand on ne sera plus obligé de passer par l'infrastructure internationale. Il en existe des mesures théoriques. Aujourd'hui, la longueur moyenne d'un trajet est d'environ 6 AS et de 15,6 routeurs. Les AS sont les autorités indépendantes de l'Internet. Quand on passe par beaucoup d'autorités, cela signifie qu'il n'y a pas d'autorité. Internet sera morcelé quand son diamètre se réduira. Le diamètre est la distance d'un extrême à l'autre par le plus court chemin. Aujourd'hui, le diamètre d'Internet est encore en expansion.

À suivre



Kavé Salamatian, Mines-ParisTech de Paris, 2011, cliché DL

Kavé Salamatian est professeur à l'Université de Savoie ainsi que professeur adjoint à l'École polytechnique fédérale de Zurich. En 2011, il a été nommé pour 5 ans membre correspondant de l'Académie des sciences de Chine, dans la section Informatique et Technologie des communications. Ses principaux domaines de recherche sont la métrologie des réseaux et leur modélisation ainsi que la théorie de l'information dans les réseaux. Il a obtenu un doctorat en 1998 à l'Université Paris-Sud 11 où il a effectué des travaux sur le codage conjoint source-canal pour la vidéoconférence sur Internet. Il est titulaire d'un DEA en informatique théorique, d'un mastère en système de communications et

Le routage, enjeu de cyberstratégie

d'un MBA, où sa thèse a porté sur la simulation de stratégie commerciale inspirée de Sun Tze. Il a travaillé dans le domaine de l'analyse de risque, et a pris plaisir à travailler comme analyste de trafic urbain avant de s'intéresser au trafic réseau. Il s'intéresse ces derniers temps à comprendre si les réseaux sont une science ou juste une distraction technologique. Il s'intéresse aussi à la cyber-stratégie et à la compréhension des enjeux du trafic et de la connectivité inter-domaine sur l'économie et la politique régionale.