Le hard du soft : la matérialité du réseau des réseaux

Dominique Boullier

Le « hard » du « soft » : la matérialité du réseau des réseaux

Par Dominique BOULLIER

Circulation Flux d'informations Fracture numérique Innovation Internet Puissance Soft power Réseaux Technologies

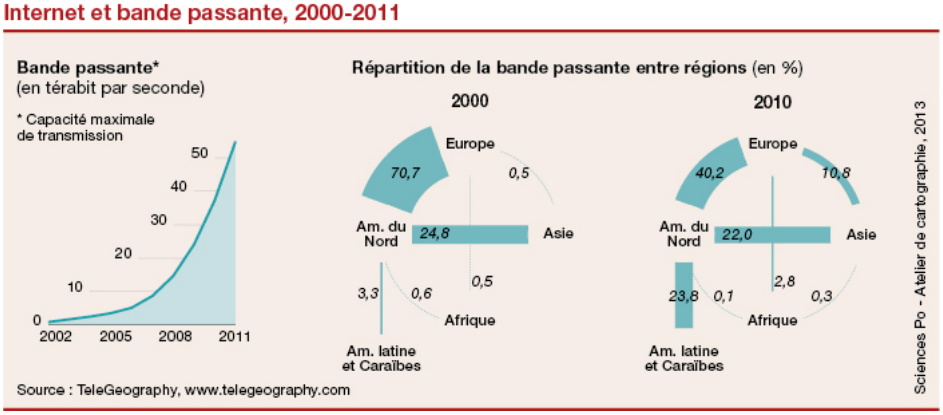
Internet, un réseau incontrôlable ? Du modèle distribué au réseau invariant d'échelle, du virtuel au *hard* des câbles et des serveurs

L'utopie majeure née avec Internet serait-elle déjà morte ? Le réseau distribué conçu comme incontrôlable aurait-il finalement succombé à diverses pressions délibérées et autres effets systémiques pour devenir aussi contrôlable que n'importe quel autre tuyau ? Ce qui se présentait comme un nouvel espace de jeux de pouvoirs marqués par le *soft* ne serait-il pas en passe de devenir tout simplement dépendant des propriétés de ses infrastructures, si *hard* et si aisément surveillées, bridées voire sabotées ?

L'histoire d'Internet reste quelque peu paradoxale quand on songe que Paul Baran, chercheur à la Rand Corporation, imagine en 1964 une structure de réseau distribué non pas dans une vision libérale visant à s'émanciper de tout contrôle mais par anticipation de l'exigence de robustesse d'un réseau sujet à d'éventuelles attaques de l'ennemi de la guerre froide et qui a déjà approché des seuils d'alerte élevés dans la période précédente. Tout réseau présentant une dépendance à un centre risque de se retrouver impuissant dès lors qu'une première frappe viserait ce centre de commandement et empêcherait la riposte qui est à la base de la doctrine de la dissuasion. Préserver la circulation des informations et des ordres militaires devient dès lors un enjeu majeur qui nécessite une forme de révolution conceptuelle puisque, à cette époque et aujourd'hui encore, les réseaux de télécommunications fonctionnent à base de centraux (commutateurs) qui sont autant de points de passage obligés et que les réseaux informatiques rattachaient des terminaux sans ressources locales à des ordinateurs dits « *mainframes* », dont ils se partageaient le temps de calcul (le temps partagé étant inventé à la même époque). Projeter un réseau distribué (et non décentralisé), c'est donc annuler les contraintes des architectures de réseau de l'époque, leur contrainte *hard*, pour anticiper une circulation d'entités le long de réseaux hétérogènes sans parcours prédéfinis mais seulement calculés localement et au fur et à mesure par optimisation des routes. Ce n'est que dix ans plus tard, à partir de 1973, que sera mise en œuvre cette vision avec l'invention du protocole de code de transfert (Transfer Code Protocol, TCP), augmenté ensuite du protocole Internet (Internet Protocol, IP), dont le nom dit bien la diversité des types de réseaux connectés et l'indifférence à leurs propriétés *hard* (filaires, radio, satellites, sous-marins). Cette distribution allait à l'encontre des projets des opérateurs de télécommunications qui prétendaient garder le contrôle de ces réseaux informatiques *via* leurs centraux avec le protocole X25 (qui vient seulement de s'éteindre en 2012 en France). Malgré leur bataille farouche et coordonnée au niveau international avec l'Union internationale des télécommunications (UIT), ces « telcos » devront petit à petit admettre leur défaite face à la plasticité d'une architecture comme celle d'Internet, fondée non sur la commutation par circuits des télécoms mais sur des paquets (issus des travaux entre autres de Louis Pouzin à l'Institut de recherche en informatique et en automatique (Iria) – ancêtre de l'Institut national de recherche en informatique et en automatique (Inria) – sur les datagrammes, aujourd'hui enfin officiellement reconnu comme l'un des fondateurs d'Internet). Dès lors, l'indépendance vis-à-vis du *hard* semblait acquise et permettait de tout connecter et d'assurer une fluidité et une plasticité extrême.

Ce fut d'ailleurs le début de la « grande peur » des autorités de contrôle de toutes sortes, particulièrement avivée en « grande peur de l'an 2000 » marquée notamment par l'effondrement de l'industrie de la musique face à une architecture *peer-to-peer* (né en 1999, Napster est contraint de fermer en 2002) qui profitait à plein du caractère distribué d'Internet. La grande peur du bug tant annoncé donnera seulement l'occasion de vérifier que le codage des années en deux chiffres constituait un choix *hard* en quelque sorte, qui pouvait faire trembler tous les systèmes à base d'électronique tant ces horloges étaient répandues partout et avec elles, le numérique. Désormais, non seulement les paquets peuvent emprunter tous les chemins offerts par les routeurs, mais chaque détenteur d'une machine peut se prétendre serveur et distribuer des contenus, dont le système *peer-to-peer* recompose les paquets après coup. A partir de 2000 s'engage donc une offensive en règle contre cette libre circulation qui aboutit à une privatisation massive de pans entiers d'Internet qui repose sur des technologies de surveillance et de recentralisation diverses. **Première altération commerciale** du caractère distribué sous le coup de la riposte généralisée des ayants droits détenteurs de la rente. Ce sont alors des protocoles de surveillance bien matériels qui sont mis en place et qui débouchent en France sur la surveillance par la Haute autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi) ou encore sur les tentatives de Deep Packet Inspection, technologie permettant d'aller vérifier le contenu des paquets transmis, pour allouer à volonté la bande passante du réseau par exemple, selon les contrats entre ayants droits.

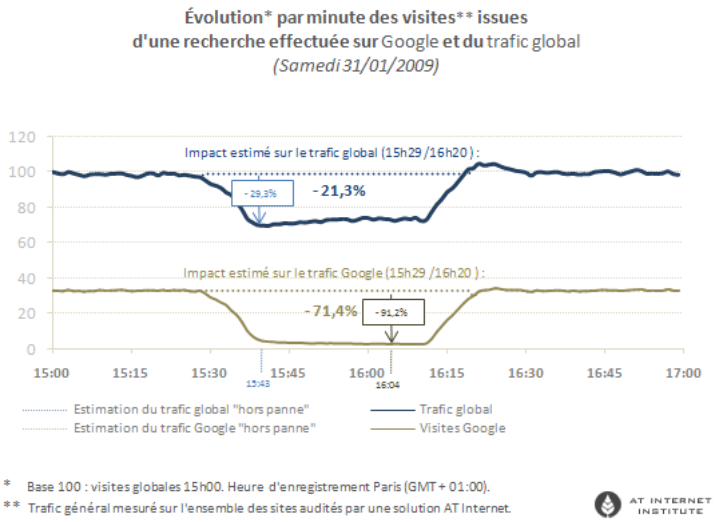
Internet et bande passante, 2000-2011



Au même moment, la « grande peur de l'an 2000 » se trouve amplifiée par le 11 septembre 2001 et la mise en évidence du caractère distribué d'une menace terroriste non réductible à un territoire donné. Dès lors, la machine sécuritaire s'emballe dans tous les pays et l'architecture fluide d'Internet devient une menace pour les Etats démocratiques, sans parler des Etats autoritaires qui avaient déjà senti auparavant la nécessité de tenir ce potentiel de communication sous haute surveillance mais en verront l'urgence avec l'émergence du web 2.0 et de ses modèles contributifs. Les attentats récents (Boston, 15 avril 2013 ; Londres, 22 mai 2013) commis par des individus isolés mais formés et reliés par Internet, nous dit-on, ne font que confirmer cet état d'esprit de soupçon vis-à-vis de l'ouverture du réseau des réseaux. Deuxième altération donc du caractère distribué du réseau, **une altération sécuritaire**, qui donne lieu à des batailles légales régulières sur les droits que s'accordent les agences de sécurité au détriment des libertés fondamentales des citoyens, et cela jusque dans le design des clés de cryptage ou des systèmes d'exploitation devant garder ou non une porte d'accès (*backdoor*) pour des raisons de sécurité nationale. Edward Snowden a révélé en juin 2013 l'entreprise de surveillance démesurée mise en place par la National Security Agency américaine sous le nom de PRISM, qui démontre si besoin était l'ampleur de la contagion sécuritaire dans l'esprit des dirigeants et des services spécialisés. Etudier l'infrastructure des réseaux et leur matérialité, c'est désormais prendre en compte tous les points d'accès matériels aux flux d'information captés par ces agences et rapatriés vers leurs centres de décision (Fort Meade près de Washington) ou de calcul (par exemple Bluffdale, Utah, capable d'héberger 5 000 milliards de Gigaoctets selon

Libération du 27 juin 2013, ou Domme en Dordogne).

Mais la « grande peur » se trouve renforcée indirectement par les effets même de la croissance de la connectivité du réseau Internet, ce que l'on peut appeler une **altération topologique**. Il est difficile d'y voir l'effet d'un plan délibéré mais il est certain que la concentration des activités des internautes autour de quelques grands nœuds, que sont par exemple Google et Facebook désormais, fait bénéficier ces entreprises d'effets de monopole qui mobilisent la majeure partie des ressources du réseau à leur profit. Mais ce phénomène, encouragé par le succès de ces offres, modifie en profondeur la structure du réseau. Internet est en effet un réseau invariant d'échelle (*scale free network*), ce qui signifie que la connectivité entre les nœuds ne se maintient pas à l'état identique lorsque le réseau croît en échelle, mais que certains nœuds attirent plus les nouveaux arrivants (« attachement préférentiel ») et créent de ce fait une connectivité plus grande avec ces nœuds déjà puissants. Ainsi, tout nouveau site web se trouvera plus rapidement connecté à Google qu'à tout autre nœud et, ce faisant, augmentera encore la centralité de Google dans tout le réseau. Dès lors, le réseau n'est plus aussi distribué qu'on le pensait à l'origine car de vrais centres se sont reconstitués par ce seul effet de réseau qui favorise la connexion aux nœuds déjà les plus attractifs. Le réseau s'en trouve fragilisé d'un point de vue stratégique puisqu'il suffirait de frapper les fermes de serveurs de Google pour le mettre sérieusement en difficulté. Ce fut d'ailleurs le cas à petite échelle le 31 janvier 2009 lors d'une panne de Google pendant quelques heures, qui montra que devant l'échec de leurs requêtes vers Google, une bonne partie des utilisateurs ne se tournait pas vers d'autres moteurs de recherche mais abandonnait carrément leur activité sur Internet, ce qui aboutit à une chute de 40 % du trafic d'Internet par le seul fait d'une panne très brève de connexion à Google.



Lire l'étude « A qui a profité le bug de Google ? » sur le site AT Internet Institute

Le réseau distribué est désormais dépendant des centres que sont les fermes de serveurs de Google ou de Facebook, certes disséminées dans le monde mais cependant bien matérielles et localisées. La fragilité d'une telle architecture est vivement ressentie mais dépend en fait de la capacité de compagnies privées supranationales comme Google à assumer leur rôle de gardien du réseau pour le bien commun et non pour leur seul bénéfice.
Ces trois éléments (commercial, sécuritaire et topologique) ont ainsi contribué à rendre visible la part prise par les infrastructures techniques, par leur maintenance et par leur contrôle. Non, tout ne circule pas en tous points sur Internet par la seule vertu des prouesses logicielles, déterritorialisées, partagées et incontrôlables. Plusieurs formes de la matérialité des réseaux sont restées incontournables et deviennent désormais explicitement l'enjeu de batailles féroces entre parties prenantes d'un ordre dont les frontières sont difficilement définissables.

Nous insisterons ici sur cinq aspects de ce *hard power* qui organise les réseaux :

1/ Les systèmes de transmission, leur diversité et leur matérialité, ce qui les rend contrôlables.

2/ Les points d'entrée dans les pays du point de vue des télécommunications : pour certains pays, seulement quelques points concentrent l'accès à toutes les communications et créent ainsi une fragilité aux attaques ou aux censures de tous types.

3/ Les serveurs, qu'ils soient routeurs des Internet Exchange Points ou regroupés dans les fermes de Google ou de Facebook ou qu'ils gèrent les noms de domaine pour la Société pour l'attribution des noms de domaine et des numéros sur Internet (Internet Corporation for Assigned Names and Numbers, ICANN, qui a succédé à l'Internet Assigned Numbers Authority, IANA, en 1998) : leur puissance et leur distribution indiquent bien des priorités et des centralités.

4/ Les grands calculateurs. La répartition mondiale de ces puissances de calcul éclaire d'un autre jour les capacités de chaque pays en matière de défense, de recherche et de supervision d'opérations majeures de contrôle.

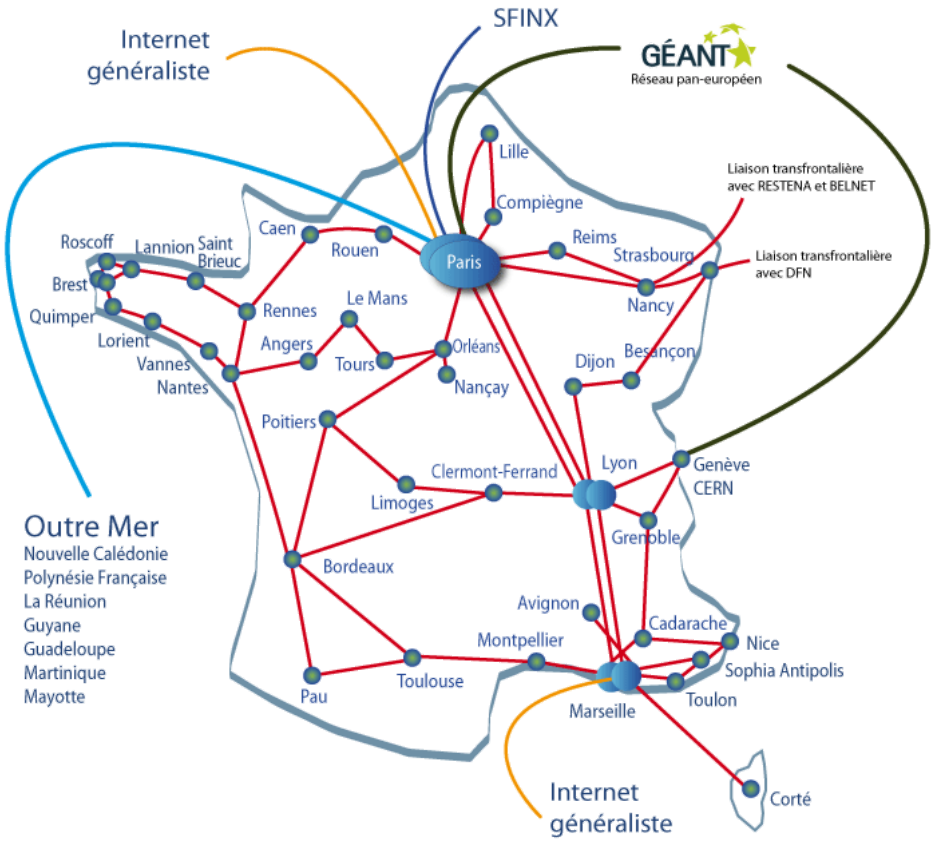
5/ Les standards pour les réseaux mobiles.

Le réseau des réseaux est un réseau de tuyaux

Qui dit Internet dit connexions entre plusieurs types de réseaux selon le même protocole. Cet aspect semble désormais tellement évident qu'on l'oublie souvent alors que dans les années 1970, chaque réseau physique pouvait avoir son protocole spécifique. La couche physique de tous les réseaux informatiques constitue la première couche du modèle OSI (Open Systems Interconnection), là où se transmettent les signaux électriques ou optiques, qui peuvent être gérés par des protocoles différents. Désormais, cette diversité matérielle est transparente pour l'utilisateur ordinaire qui ne sait plus si ses communications, et plus exactement les paquets qui la composent, empruntent des réseaux filaires (en paire de cuivre, en Ethernet, en fibre optique ou en coaxial), sans fil, satellitaires ou des câbles sous-marins. Il devient dès lors difficile de faire la carte de ces réseaux qui ont des propriétés techniques et matérielles si différentes. Pourtant, les investisseurs ne s'y trompent pas. La croissance du haut débit et l'extension de la connectivité de continents entiers dépendent du déploiement de ces infrastructures. Certaines sont partagées, bénéficient même de subventions publiques et peuvent alors être décrites publiquement ; mais bon nombre de réseaux déployés par les opérateurs constituent des secrets industriels qu'ils ne veulent pas divulguer par crainte de la concurrence. Ainsi la dernière carte publiée des réseaux de fibres optiques opérés par Orange en France date de 2007 et n'est pas mise à jour publiquement (à la différence de la carte de couverture haut débit), et cela d'autant moins que le débat fait rage sur le partage des charges d'investissement dans le futur réseau haut débit à base de fibre optique. Le débat public devient particulièrement difficile dans ces situations de rétention d'information pour des infrastructures qui constituent pourtant un bien commun, si ce n'est public : la carte qui rend visible ces réseaux devient ainsi une ressource stratégique.

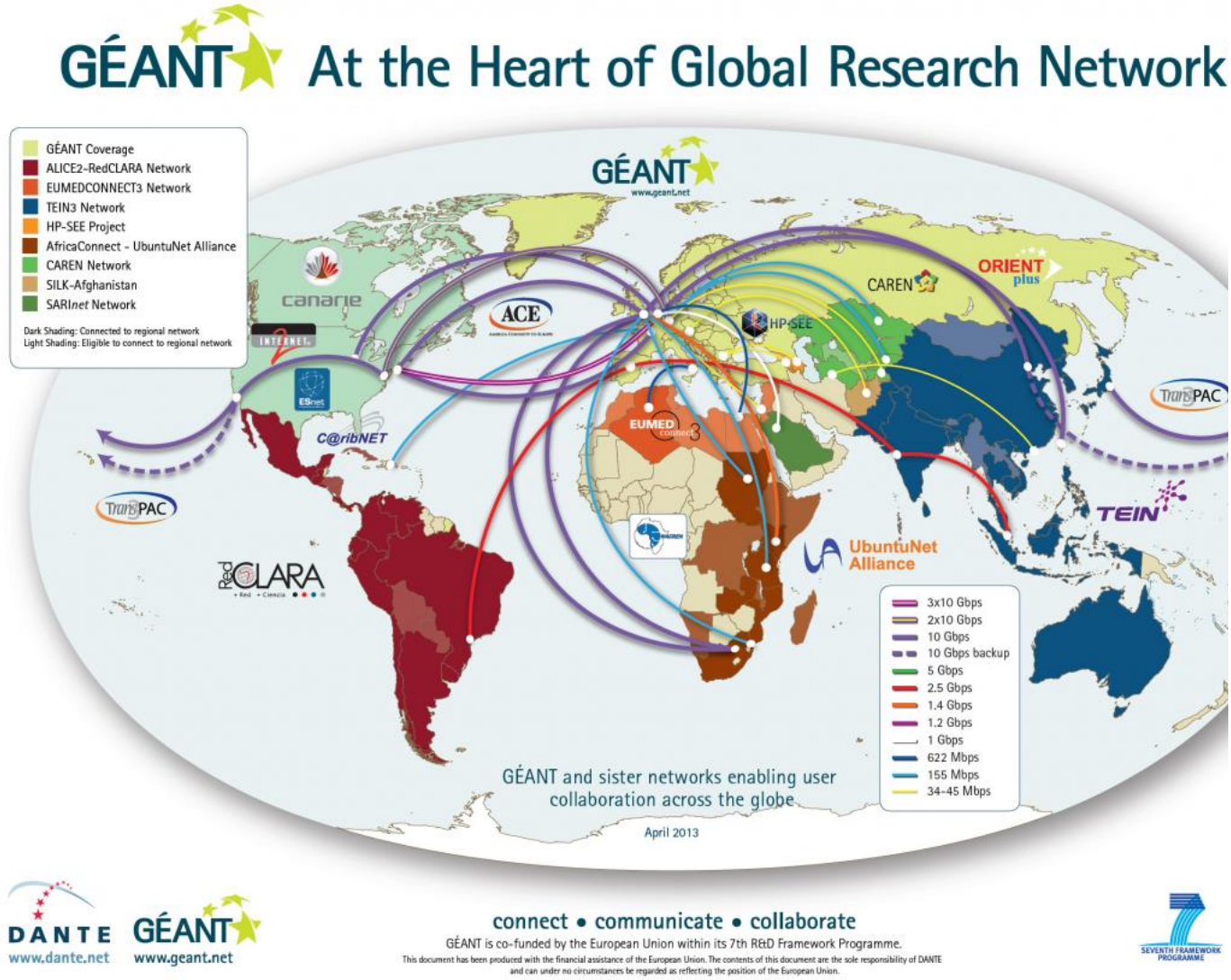
Il est plus aisé d'obtenir la carte des dorsales internet (*backbones*) des réseaux nationaux et internationaux, lorsqu'ils sont maintenus par des opérateurs publics que sont par exemple les réseaux académiques, qui, rappelons-le, sont aussi à l'origine du principe même d'Internet, en même temps que les militaires.

Ainsi, la carte des dorsales françaises est publiée par le Réseau national de télécommunications pour la technologie, l'enseignement et la recherche (Renater) et il est même possible de consulter une application dynamique qui permet de visualiser en direct l'activité de ces réseaux. Renater est un groupement d'intérêt public (GIP) créé en 1992 qui regroupe les grands organismes de recherche et les ministères de l'Éducation nationale et de l'Enseignement supérieur et de la recherche. Il est l'opérateur du réseau de recherche national qui est lui-même connecté à Internet *via* le point d'échange de trafic SFINX (Service For French Internet Echange Point). Depuis le début des années 2000, le GIP a pris en charge le déploiement de fibre noire (c'est-à-dire brute, sans formatage par un opérateur donné) pour constituer un réseau de 8 000 km à très haut débit (au moins 10 Gbit).



Voir la carte du réseau sur le site de Renater

Tous les réseaux à très haut débit de la recherche et de l'enseignement supérieur sont par ailleurs reliés entre eux et constituent une infrastructure de coopération essentielle pour les chercheurs. Le réseau Gigabit European Academic Network (GEANT) et le programme d'activités associées (GN3) sont cofinancés par l'Union européenne dans le cadre du 7e programme cadre de recherche et développement (PCRD) et les réseaux nationaux d'enseignement et de recherche (NRENs).

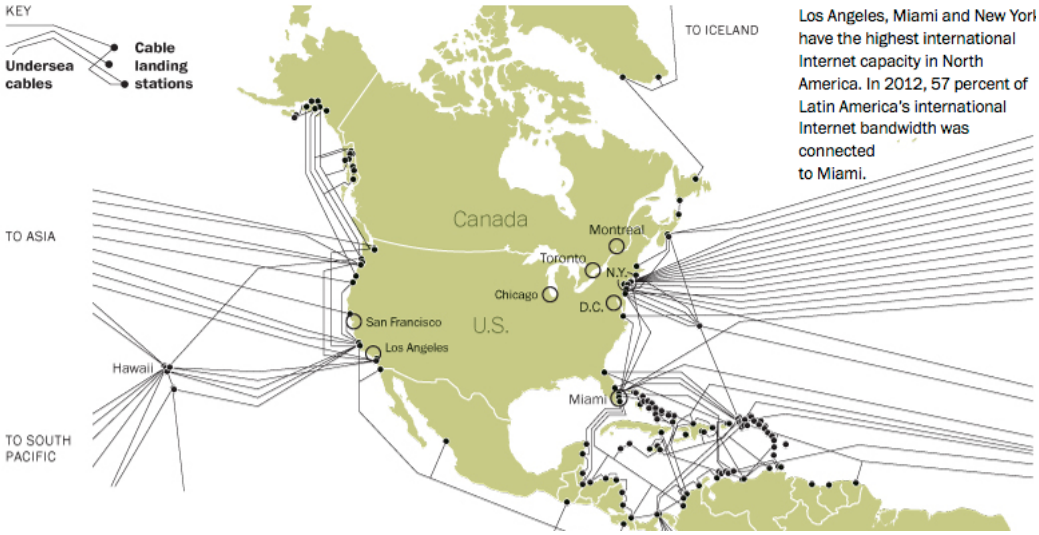


Voir les cartes du réseau Gigabit European Academic Network (GEANT)

Les câbles sous-marins restent les infrastructures décisives car les plus fiables pour tous ces types de réseaux. La pose des premiers câbles transatlantiques fait partie des avancées décisives pour les télécommunications dès le début de leur histoire. Après les premiers essais en 1838, le premier câble fonctionnel fut posé en 1851 entre le cap Gris-Nez et Southampton et servit avant tout à transmettre par télégraphe les cours des bourses. Le premier câble transatlantique fut posé en 1858, le premier câble transpacifique en 1902, tous deux des câbles analogiques. Le premier câble à fibres optiques fut posé en 1988 et les capacités de transmission augmentèrent alors rapidement, avec un multiplexage permettant de faire passer plusieurs signaux sur la même couleur de la fibre (plus de 100 couleurs). Les compagnies de câbleurs et les propriétaires de ces câbles sont peu nombreux car les investissements sont élevés, mais la rentabilité est assurée. Le développement de la carte des câbles reflète clairement les priorités des investissements selon les marchés de télécommunications solvables, même si certains tracés sont aussi liés à des enjeux géostratégiques. Ainsi que le montre la carte, l'Afrique est en train de rattraper son retard et ces ressources peuvent jouer un grand rôle dans l'intégration aux échanges économiques mondiaux (services délocalisés, compétences locales connectées aux centres, etc.). Les points d'entrée eux-mêmes gagnent un avantage stratégique tant que le reste du réseau terrestre n'est pas développé au même niveau.

Diaporama interactif
Cliquer sur la flèche pour commencer

Il est désormais reconnu que les points d'entrée constituent les meilleurs accès pour ceux qui veulent contrôler les données de ces réseaux. Les Etats-Unis possèdent une grande quantité de points d'entrée des câbles sous-marins (voir ci-dessous) mais une très grande partie du trafic européen avec l'Amérique du Nord transite par trois points d'entrée, situés en Cornouaille au Royaume-Uni : Porthcurno, le plus ancien (Blum 2012) (et combiné à Sennen Cove, Skewjack et Whitesand Bay), Highbridge et Bude/Widemouth Bay, le plus important.



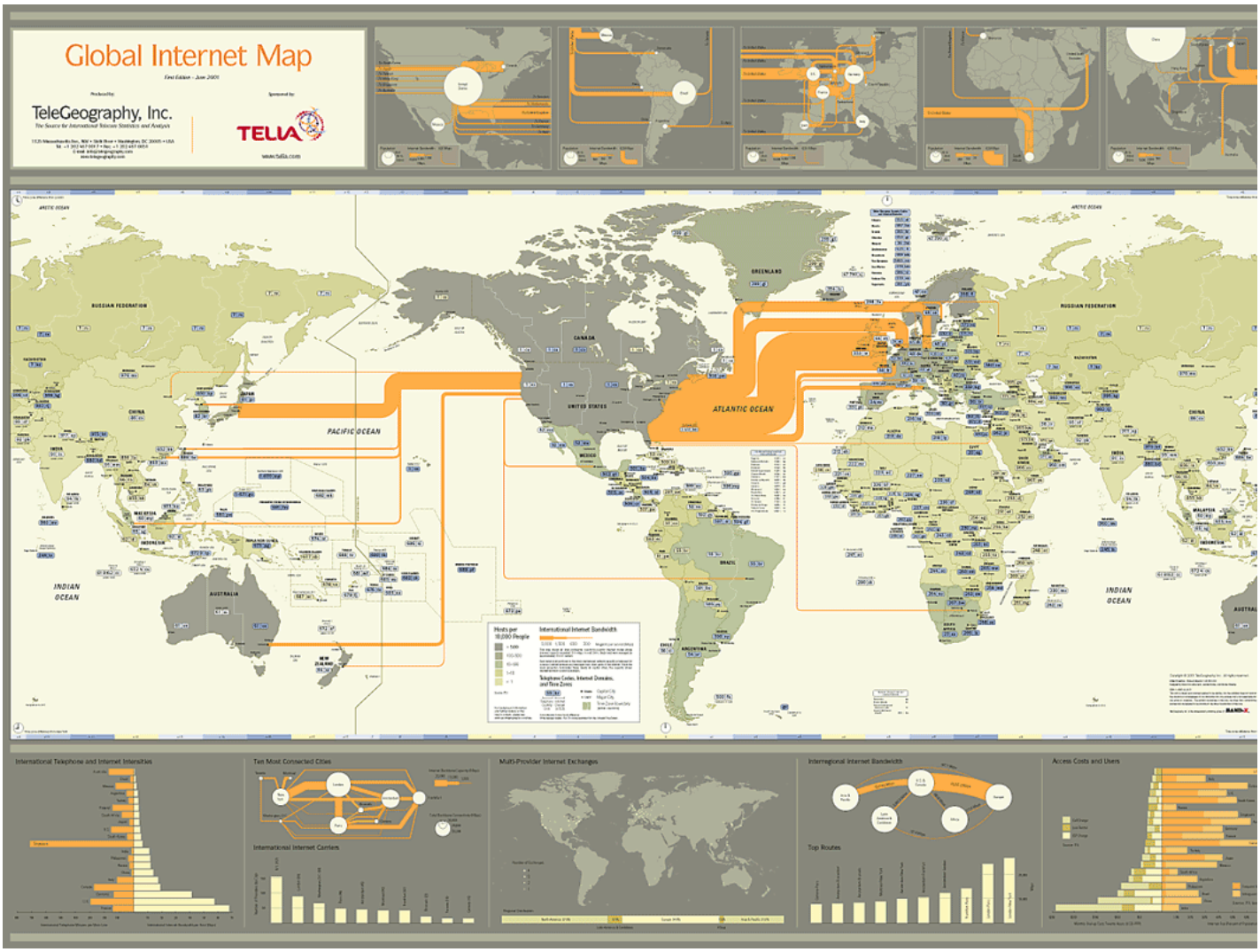
Lire l'article « A connected world » de Todd Lindeman
sur le site du *Washington Post*

La pose de câbles peut d'ailleurs devenir l'objet de batailles commerciales et sécuritaires importantes, qui portent moins sur le contrôle des câbles eux-mêmes que sur les composants technologiques qu'ils comportent, comme en témoigne un conflit récent entre les Etats-Unis et un opérateur chinois Huawei :

> « A la mi-février 2013, la construction d'un câble sous-marin de 4 600 km entre Londres et New Yorkpour le trading automatisé a été 'mise en pause'. L'entreprise responsable, Hibernia Networks, a dû arrêter le projet à cause des opérateurs américains, qui déclarent perdre leurs contrats avec le gouvernement fédéral si le déploiement est mené à bien. La raison ? Huawei était chargé de fournir les câbles de fibre optique et du matériel de transmission et d'amplification, ce qui aurait été jugé inacceptable par les autorités américaines. » (*Le Monde*, 24 avril 2013)

Ainsi, lors du récent scandale Snowden/NSA/Prism, le *Washington Post* du 7 juillet 2013 a révélé que les Etats-Unis ont tout fait pour maintenir un contrôle stratégique sur les firmes de câbles, grâce à une cellule spéciale « Team Telecom », qui a notamment fait capoter un projet de rachat de la société Global Crossing par une firme de Hong Kong en 2003. La compagnie Singapore Technologies Telemedia qui racheta finalement l'entreprise dut accepter des règles très strictes pour garantir que les postes principaux restent occupés par des citoyens américains et que la NSA puissent avoir accès aux données transitant sur les câbles.

Lorsque l'on tente de cartographier les trafics sur ces réseaux, les asymétries apparaissent très clairement. Elles peuvent être trompeuses en mettant toujours en lumière la domination écrasante des échanges entre Europe et Amérique du Nord. Les raisons économiques et historiques suffisent à en rendre compte. Cependant, c'est à la vitesse de déploiement des infrastructures autour des pays émergents et au trafic qui s'y développe que l'on devrait être plus attentif (et les données ne sont pas si aisées à trouver sur ce point) car on mesurerait alors que des rattrapages accélérés sont en cours.

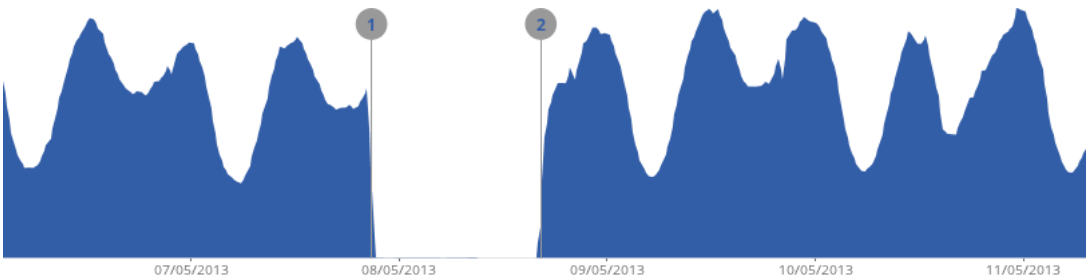


Quelques exemples de cartographie des trafics
sur le site *Atomic Toasters*

Les cartes de couverture par les réseaux, notamment pour les technologies mobiles, présentent l'inconvénient d'être extrêmement variables, parfois présentées commercialement, et elles ne permettent pas d'identifier par exemple un réseau d'antennes et leur localisation. Ce sont cependant de bonnes approximations de l'équipement puisque les portées de ces antennes sont limitées. Le site Sensorly (http://www.sensorly.com/fr) recense ainsi près de 250 réseaux dans le monde, avec une répartition inégale, qui permet de vérifier dynamiquement les couvertures par opérateur et par type de réseau (2G/3G/4G/wifi) selon les pays.

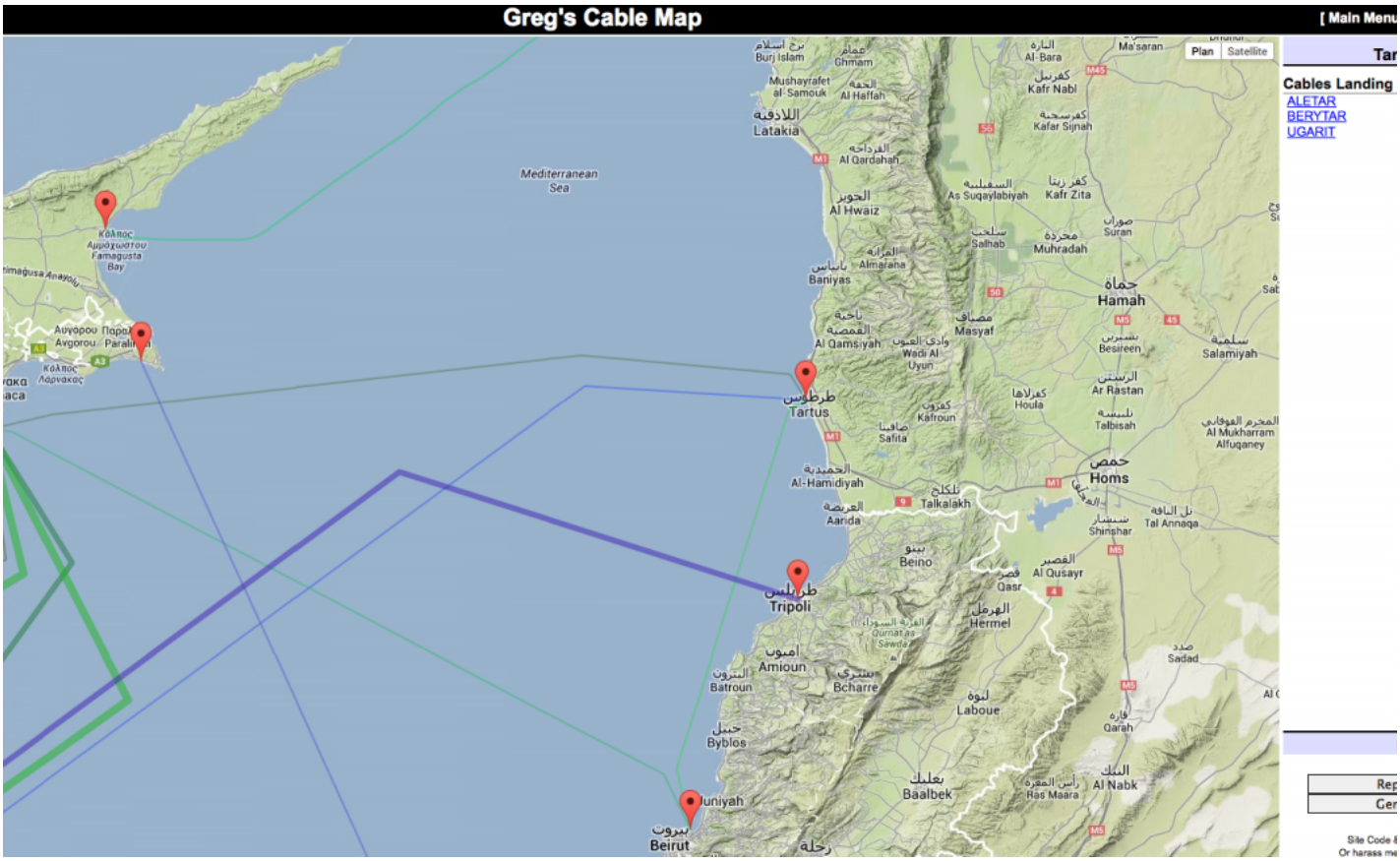
Les points d'entrée par pays

L'attention portée à la matérialité des réseaux et à toutes les infrastructures qui les font tenir crée, nous l'avons vu, des inégalités d'accès très nettes qui ne font que redoubler d'autres inégalités. Mais la rareté des câbles, par exemple, peut à elle seule créer les conditions de fragilité d'un pays ou faciliter le contrôle par les régimes politiques non démocratiques. En France, la diversité des points d'accès, des opérateurs et des propriétaires des câbles rend de fait improbable toute perte de connectivité avec Internet. Ce n'est pas le cas pour des pays comme la Syrie qui a connu en novembre 2012 et en mai 2013, des coupures de quelques jours, qui ont parfois touché toutes les télécommunications.



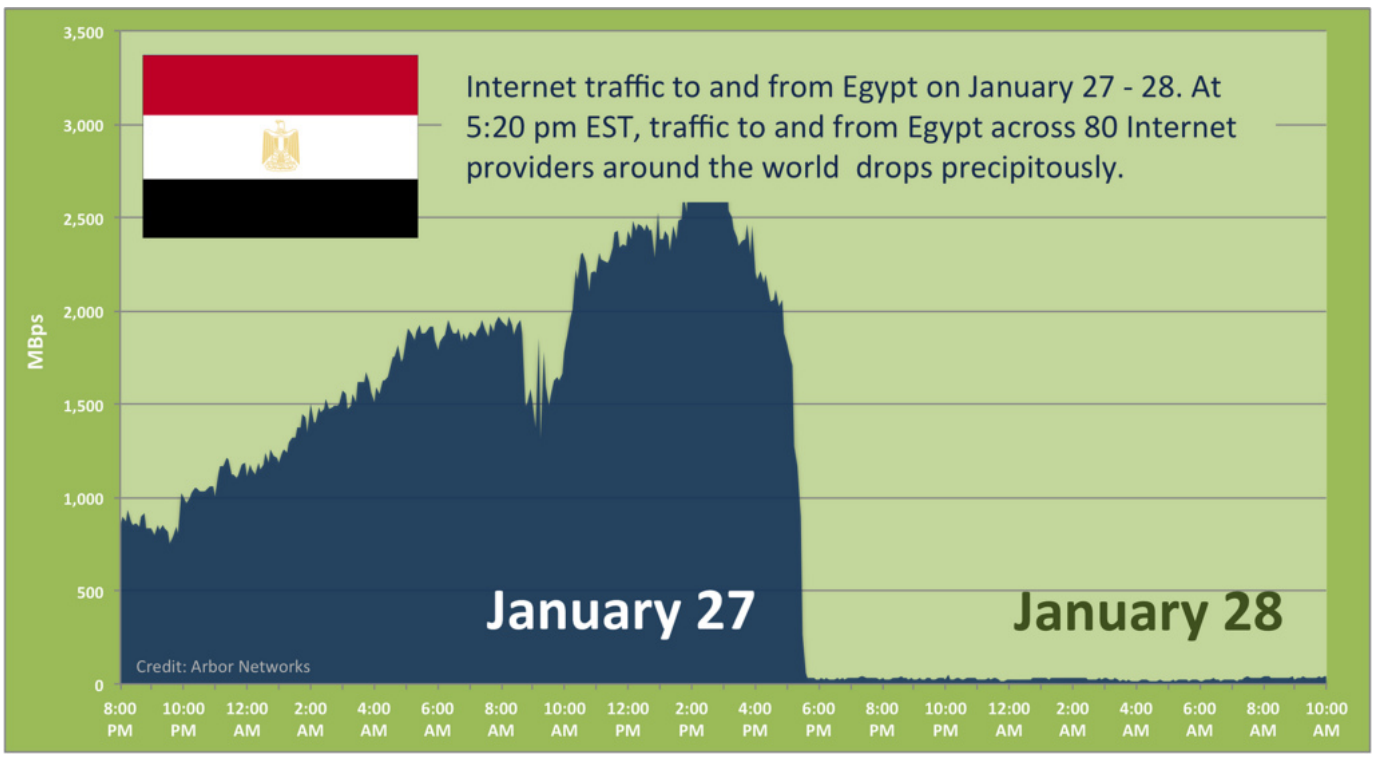
Voir les coupures en Syrie consignées par Google

La brutalité de ces chutes laisse supposer qu'il s'agissait d'une action délibérée car même la Syrie possède quatre câbles – le câble Aletar (relié à Alexandrie en Egypte), Berytar (relié à Beyrouth), Alasia et Ugarit (relié à Pentaskhinos à Chypre) – qui arrivent tous à Tartus et auraient pu, l'un ou l'autre, maintenir un certain trafic en cas d'incident technique.



Source : www.cablemap.info/

Cette fragilité est donc une ressource aux mains des régimes non démocratiques et tous les pays arabes ont connu des épisodes de coupure d'Internet au moment de leurs révolutions. Elle fut particulièrement longue en Egypte (cinq jours) et n'a pu être surmontée pendant cette période de *blackout* que grâce à l'intervention de hackers comme ceux de Telecom-X utilisant les lignes téléphoniques et des modems anciens. Pourtant, la question des accès physiques restreints ne semble pas avoir été le seul facteur dans cette opération. L'Egypte comptait quatre opérateurs à l'époque (Link Egypt, Vodafone/Raya, Telecom Egypt et Etisalat Misr) qui ont tous subi les décisions du régime et ont de fait fermé les accès (voir *infra*).

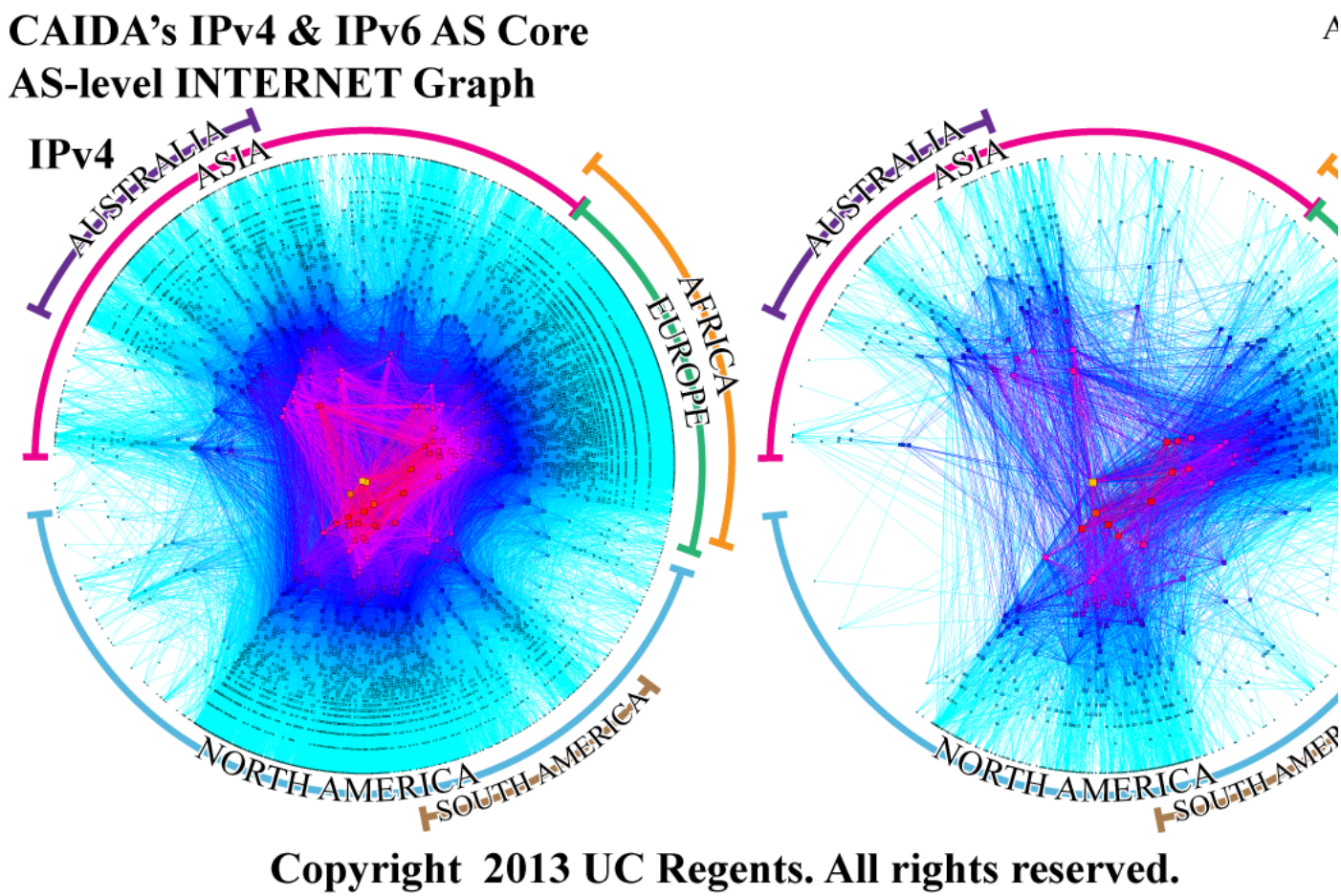


Source : http://www.arbornetworks.com

La Chine peut sembler moins vulnérable puisque quatre grands points d'accès de câbles sous-marins peuvent être identifiés : Qingdao, Shanghai, Shantou et Hong Kong. Cependant, dans ce cas, la volonté de contrôle d'Internet est jugée si cruciale que ce que l'on appelle le Great Firewall (grande muraille pare-feu) fonctionne en permanence avec une armée de plusieurs dizaines de milliers de contrôleurs qui peuvent fermer les accès à certains sites à volonté. Le contrôle des infrastructures est certes plus efficace mais il devient si brutal qu'il met en péril tous les échanges avec l'extérieur, ce qui est devenu intenable sur plusieurs jours, même pour une dictature. Dès lors, les contrôles doivent opérer grâce à des filtres et des technologies de surveillance dont, par exemple, la société française Amesys s'est fait une spécialité, mais qui demandent dans tous les cas une force de travail humaine considérable (e.g. interdiction de certains mots sur les moteurs de recherche par exemple, ce qui demande une mise à jour permanente).

Il existe donc bien des frontières créées par cette matérialité des accès à des réseaux physiques mais leur contrôle est encore logique, au sens où ce sont des instructions qui sont habituellement échangées par-delà les frontières que l'on peut interrompre à volonté. Le protocole en question s'appelle Border Gateway Protocol (BGP) mais n'est pas censé faire référence à des frontières étatiques. En effet, il s'agit d'un protocole de routage du trafic entre ce qu'on appelle des *Autonomous Systems* (AS) qui peuvent être des fournisseurs d'accès. Cependant dans les pays non démocratiques, les fournisseurs d'accès sont peu nombreux et contrôlés par l'Etat, ce qui aboutit en fait à créer un AS pour tout le pays. Les connexions entre fournisseurs d'accès (et donc vers l'extérieur d'un pays dans le cas restreint que l'on évoque ici) reposent sur des annonces réciproques sur les blocs d'adresses IP qu'un fournisseur d'accès souhaite utiliser. Dès lors qu'un fournisseur ne les demande plus, les échanges *via* ce BGP s'arrêtent. Selon le même protocole mais avec une visée différente, Pakistan Telecom, appliquant une décision du gouvernement pakistanais contre YouTube, avait annoncé en février 2008 à tous les routeurs des fournisseurs d'accès qu'il était la meilleure route pour YouTube, ce qui a aspiré le trafic et pendant deux heures a bloqué YouTube par saturation dans le monde entier.

La carte de ces AS, qui correspondent souvent à des Internet Service Provider (ISP), et de leur connectivité réciproque est sans doute l'approximation la plus juste de la topologie actuelle du réseau, car elle a été construite sur l'enregistrement des routes les plus fréquentées en 2013 et permet ainsi de voir les émergences de centralité autour de certains AS. Il s'agit bien de topologie fondée sur des calculs de graphes et non de topographie ou de géographie. La localisation spatiale de ces AS est cependant possible après coup et permet de voir le rôle central de ces opérateurs de câbles sous-marins déjà évoqués tels que Tata, Global Crossing ou Level3.



Voir les graphes réalisés
par la Cooperative Association for Internet Data Analysis (CAIDA)

Une autre ressource pour limiter ces entrées consiste à fermer certains ports, c'est-à-dire certains types d'accès selon des protocoles particuliers (par exemple le port 80 pour l'accès au web en http). Ainsi l'Iran est-il désormais coupé du monde pour tous les Virtual Private Network (VPN, port 1723), à l'instar de la Chine, et tous les protocoles sécurisés comme https (port 443), et il prétend ainsi proposer depuis septembre 2012 un « réseau national » de qualité de niveau ADSL tout en réduisant les débits pour les accès au reste d'Internet. Ces ports sont la couche transport du modèle OSI mais sont en fait de type logiciel.

Ainsi, les frontières techniques n'ont à première vue pas de sens sur Internet. Pourtant, elles sont seulement perméables et dès lors que dans un pays donné, les pouvoirs techniques sont concentrés chez un opérateur dépendant de l'Etat, de nombreux dispositifs existent pour restreindre les accès. Ce n'est donc pas seulement la multiplicité des points d'accès physiques mais la diversité des opérateurs qui peut rendre le contrôle plus difficile.

Les serveurs : points d'échange Internet et routeurs des noms de domaine

Nous venons d'évoquer les routeurs : en effet, tout découpage de l'infrastructure entre réseaux/serveurs/protocoles/services est toujours quelque peu artificiel car les uns ne fonctionnent pas sans les autres. Cependant, dans cet article, nous avons choisi de mettre en avant les propriétés matérielles de ces réseaux. Les serveurs, qui sont les nœuds de ces réseaux, sont donc essentiels à leur activité. En théorie, comme nous l'avons dit, une architecture distribuée permet l'aiguillage des paquets sur des routes multiples. Cependant, comme le montrait le cas du BGP, les serveurs doivent calculer et optimiser les routes, et de ce fait, leurs capacités et leur répartition jouent un rôle essentiel pour rendre certaines routes très performantes et d'autres moins. C'est le rôle des Internet Exchange Point, qui constituent autant de lieux physiques où des routeurs sont alignés en rack dans des armoires par centaines, comme le décrit très bien Andrew Blum (2012). Ils sont identifiés le plus souvent sous un nom se terminant par IX ou INX, comme les plus importants en Europe : LINX (London Internet Exchange), DE-CIX (Deutscher Commercial internet Exchange), AMS-IX (Amsterdam Internet Exchange ou SFINX déjà évoqué. Ils sont situés au plus près des grands consommateurs de données, car la distance joue un rôle essentiel dans la vitesse du trafic, devenue si cruciale lorsque les transactions financières se jouent à la milliseconde. La carte géographique suivante donne la distribution spatiale de ces IXP, très révélatrice du trafic de certains pays (voir précédemment pour la carte topologique).

Voir la carte de la distribution spatiale des IXP
sur le site http://www.datacentermap.com

Nous nous intéressons maintenant aux serveurs DNS (Domain Name Services) qui constituent un premier tri dans l'orientation des paquets, selon leur adresse IP de destination. Les noms de domaine que l'on appelle TLD (Top Level Domain) sont répartis entre les « .com » et quantité d'autres domaines, dont les domaines nationaux que sont les « .fr », « .de », etc., que l'on appelle ccTLD (country code). Leur stabilisation par Jon Postel (RFC 1591 en 1994) se fonde en réalité sur la reprise des codes ISO3166-1 destinés à l'union postale internationale (avec adaptations : « .uk » et non « .gb ») et s'affirme volontiers agnostique sur ce qu'est un pays ou non. De ce fait, certains domaines de communautés linguistiques ou de régions non reconnues dans l'ISO n'avaient pas d'existence non plus comme extensions sur Internet. L'ICANN est l'association non lucrative de droit californien qui gère tous ces domaines pour l'Internet mondial. En 2011, elle a ouvert les TLD à des communautés comme la Catalogne (« .cat ») sous certaines conditions d'activités internationales, de nombre de locuteurs, de capacités financières à maintenir le domaine, etc. Plus récemment, lors d'un mouvement généralisé d'ouverture des TLD par l'ICANN, la Bretagne a obtenu son « .bzh », alors qu'elle ne correspond pas aux mêmes critères (deux langues, breton et gallo par exemple) et Paris a également obtenue son « .paris ». On mesure l'étrangeté d'un système international géré par une association de droit californien qui peut faire exister ou non des communautés « nationales » sous forme d'extensions TLD.

Or, cette orientation repose sur un système de serveurs répartis dans le monde qui sont cruciaux pour l'activité d'Internet puisque c'est le premier élément de l'adresse qui va servir à orienter les messages en transformant l'adresse lisible sur la barre de nos navigateurs en adresse IP. Les treize serveurs de noms racines sont répartis de A à M mais, contrairement à ce qu'on a parfois laissé croire en montrant la localisation de dix serveurs aux Etats-Unis sur les treize, ces serveurs ont en fait de multiples instances locales réparties dans le monde de façon à optimiser le routage (soit 365 serveurs fin 2012).

Ainsi, le serveur L est utilisé et géré directement par l'ICANN mais présente le plus d'instances démultipliées dans le monde (143). Verisign gère le « .com » (donc la plupart des services commerciaux) en utilisant les serveurs A et J, qui sont aussi distribués (huit aux Etats-Unis pour le A et soixante-dix pour le J dans le monde entier). La distribution géographique de ces serveurs reflète clairement l'écart entre pays dans leur usage d'Internet mais on peut aussi considérer qu'elle le fait persister en ralentissant certains accès puisque le passage par ces serveurs est obligatoire (en réalité, pour la plupart de nos requêtes, la route est enregistrée en cache dès lors qu'elle est fréquente).

Situé au centre de Miami, le Network Access Point de Verizon-Terremark héberge l'un des serveurs racines K du DNS.
Source : *Miami Herald* Blog

Le cas du DNS chinois

Voir la carte sur le site http://www.root-servers.org/

Sur cette carte, il est aisé de constater le quasi-désert chinois en matière de serveurs DNS, alors que la Chine démontre une croissance très élevée de son trafic Internet. En réalité, la Chine a décidé le 1er septembre 2006 de se couper du système de DNS géré par l'ICANN et de créer le sien propre. Le conflit était né entre autres de l'incapacité de l'ICANN à gérer d'autres caractères que l'alphabet latin pour ses adresses, évolution réalisée seulement à partir de 2008. La Chine permet cependant l'accès à des TLD de l'ICANN (« .com », « .net » par exemple) à partir de son DNS mais uniquement après avoir aspiré et contrôlé ces sites. Cela a permis en tous cas à la Chine de créer autant d'extensions qu'elle le souhaitait alors que tous les autres services de tous les pays sont tributaires des procédures de l'ICANN, qui ne se sont ouvertes que récemment. Ce qui veut dire que l'architecture supposée universelle d'Internet s'est radicalement fracturée en perdant son système d'orientation commun, géré il est vrai par une instance « internationale de droit californien » dont même la Commission européenne a contesté la légitimité. Le risque d'une répétition du même séparatisme dans d'autres pays s'est avéré infondé pour l'instant mais la faiblesse légale de l'institution ICANN peut donner lieu à d'autres tentatives.

Les fermes de serveurs des nœuds principaux

Les grands nœuds d'Internet, ceux qui attirent le plus de trafic, ont radicalement modifié la structure même du réseau des réseaux au point de faire quasiment disparaître son principe distribué, pourrait-on dire. Les firmes comme Apple, Google, Facebook, Amazon (dites « la bande des quatre ») ont besoin de garantir cet accès permanent et immédiat qu'elles promettent, qui a fait la différence de Google dès son apparition, vitesse qui reste l'obsession de son PDG. Qui dit vitesse dit capacité des serveurs à traiter toutes les requêtes en quelques millisecondes. Leur nombre importe dans ce cas et c'est pour cela que des « fermes de serveurs » sont désormais mises en place par ces grandes firmes. Mais la distance joue aussi un rôle et c'est pourquoi ces serveurs doivent être distribués au plus près des territoires des demandes. La carte des fermes de serveurs de Google donne ainsi une autre vision de la géographie d'Internet et de la répartition de ses usages entre les pays.

Source : Google

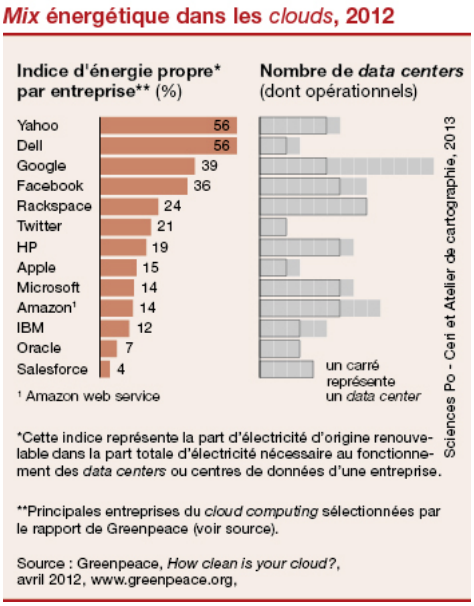
Une autre version de cette carte donne d'autres informations.

Source : WebActus

L'apparence de ces fermes de serveurs a tout de l'usine traditionnelle, notamment par ces tours de refroidissement puisque l'eau reste la ressource essentielle pour éviter la surchauffe de toutes ces machines.

La ferme de serveurs de Dublin

Les coûts énergétiques de cette centralisation de toute l'orientation d'Internet sur une seule firme (comme pour les autres grandes firmes) ne doivent pas être oubliés. Ainsi, Greenpeace a publié le mix énergétique de chacun de ces centres pour les grandes firmes du numérique.



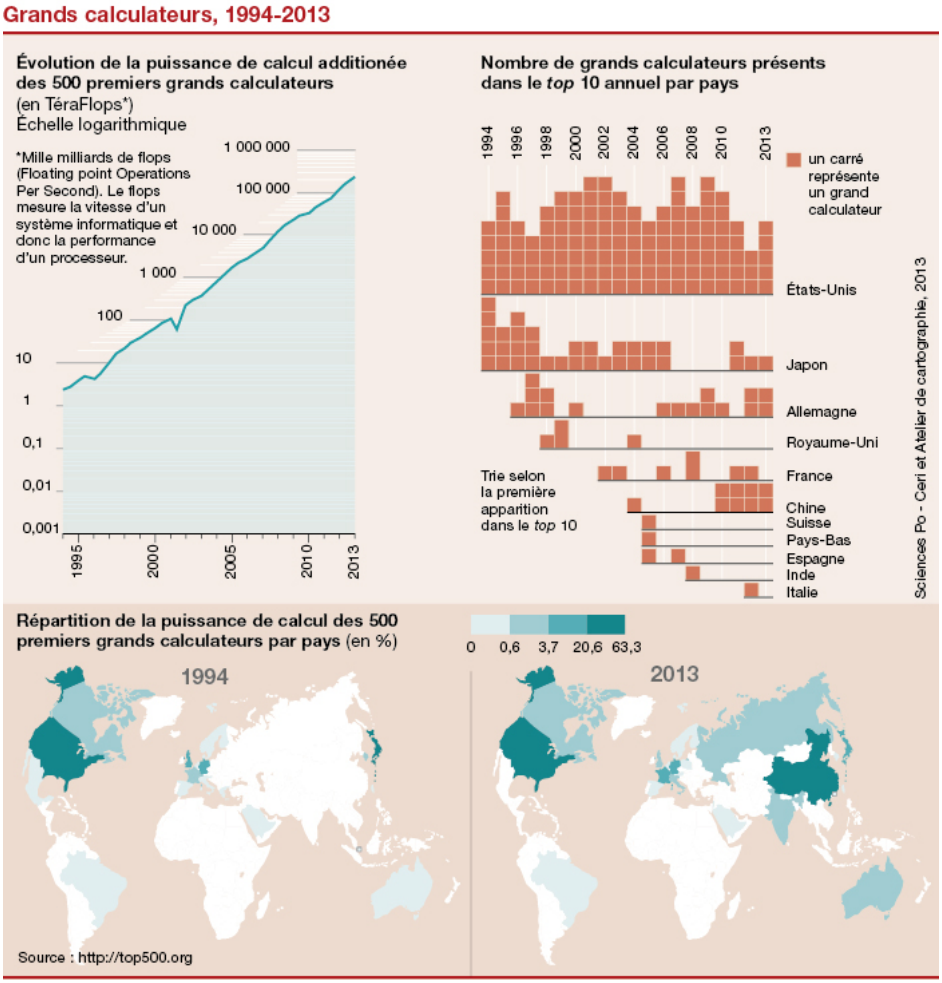
Grâce à ces chiffres, il n'est plus possible de s'affranchir de la matérialité de ces technologies de l'immatériel. Car le silicium est certes abondant à la surface de la terre, mais l'électricité reste la condition de fonctionnement de tout le système et doit encore être produite, dans des conditions non soutenables le plus souvent. Le mouvement en faveur du Green IT comporte ce volet d'optimisation des performances environnementales de toutes ces technologies mais l'architecture même du réseau et sa centralisation récente à travers la puissance d'attraction de quelques firmes contribuent à rendre plus difficile le maintien du caractère distribué et économe en énergie qu'on pouvait imaginer pour Internet.

L'estimation de la proximité nécessaire de chacune de ces fermes de serveurs avec un bassin de clientèle est une décision politique contrôlée par ces firmes selon des critères de rentabilité multiples. Dès lors, la proximité peut être toute relative, puisque ces firmes jouent encore sur des économies d'échelle que l'on croyait réservées à l'économie industrielle. Amazon possède ainsi quatre zones de serveurs qui peuvent traiter tous les pays du monde. La carte de cette répartition est intéressante : Californie du Nord (us-west-1), Virginie du Nord (us-east-1), Irlande (eu-west-1) et Singapour (ap-southeast-1).

Source : http://www.turnkeylinux.org

Les grands calculateurs

Une autre dimension matérielle des infrastructures informatiques en réseaux qu'il convient de ne pas oublier repose sur la distribution des puissances de calcul entre les pays dans le monde et les nouvelles architectures de calcul qui émergent. Les grands calculateurs ont une histoire mais aussi une géographie. Dès les années 1940, les grands ordinateurs ont été localisés sur la côte est des Etats-Unis, là où étaient les chercheurs, et notamment à Cambridge (MA). Le rôle de ces grands calculateurs était décisif pour les calculs balistiques par exemple mais aussi pour des calculs de sismologie destinés à repérer les essais nucléaires russes par exemple, puis pour les opérations spatiales de tous types. Tous ces développements militaires ont cependant créé les conditions pour mettre à disposition des chercheurs, mais aussi des industries privées, des capacités considérables. L'écart entre les Etats-Unis et le reste du monde est sur ce plan très frappant. Le Berkeley Open Infrastructure for Network Computing (BOINC) tient ce calcul à jour. Bien qu'une localisation précise ne soit pas disponible dans chaque pays, la géographie est déjà très parlante. Les nouveaux grands supercalculateurs comme les Cray sont toujours aussi inégalement répartis mais il faut souligner à quel point la Chine notamment cherche à rattraper son retard dans ce domaine et a acquis un Cray récemment. Cette géographie est à surveiller car elle est un bon indice des inégalités de fond, indépendante des usages et de la connectivité mais plus directement décisive pour les capacités de recherche militaires et industrielles de pointe. La taille de ces calculateurs a considérablement diminué mais leur coût reste toujours très élevé. Les Etats sont dans ce cas des opérateurs incontournables.



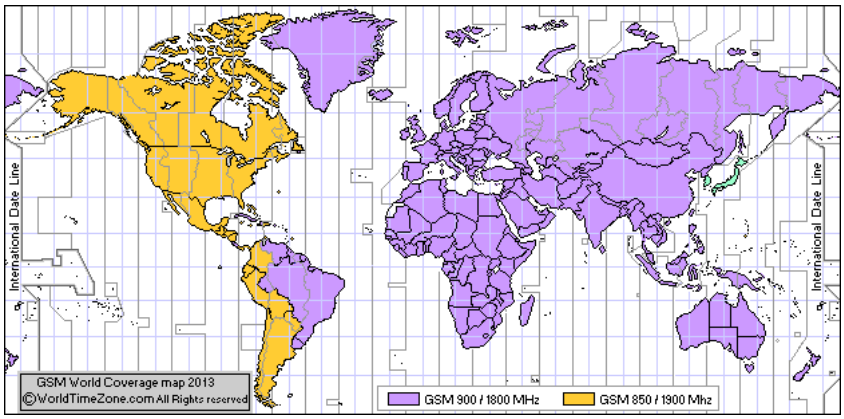
Voir également la carte réalisée par le New York Times

Cependant, ces capacités de calcul bénéficient désormais des effets de réseaux. Dès lors que les infrastructures que nous avons décrites sont fiables et bien distribuées dans un territoire, voire dans le monde entier, il devient possible de répartir de travail de calcul entre machines de plus faibles capacités mais disponibles alternativement, par exemple la nuit. Cette démarche n'est pas seulement le fait de hackers adeptes du partage, de la coopération et de la distribution par idéologie : eux-mêmes et tous les grands demandeurs de calculs scientifiques notamment ont compris l'efficacité remarquable de ces architectures distribuées que l'on appelle les *grids* (dont on peut trouver une liste sur http://distributedcomputing.info/). Dans certains cas, il s'agit de centres de recherche qui mettent leurs machines en réseaux pendant des jours et des nuits sur des calculs nécessaires à leurs projets. Par définition, ces réseaux ne sont pas cartographiés car ils sont provisoires ; leur localisation importe peu et les machines potentiellement toutes reliées entre elles peuvent participer à des degrés divers. Dans d'autres cas, ce sont des internautes ordinaires qui sont sollicités pour mettre leur ordinateur à disposition, voire pour participer à des calculs et à des codages (*volunteer computing*, comme le BOINC par exemple ou encore à l'image du projet Clickworkers réalisé par la NASA de 2000 à 2007 pour son codage des images de cratères sur Mars). Dans d'autres cas encore, ce sont des architectures industrielles de pilotage de ressources énergétiques partagées qui deviennent la clé de la gestion d'un réseau électrique par exemple. Ce dernier cas a été popularisé sous le nom de *smart grids*, qui constituent l'un des projets phares de toute *smart city*. Une autre géographie des villes se dessine ainsi (inventaires et cartes disponibles sur http://www.smartgrids-cre.fr/), mais potentiellement, c'est tout le réseau électrique d'un Etat et des Etats voisins qui coopèrent en matière d'énergie qui peut prendre une nouvelle forme.

Les standards pour les réseaux mobiles

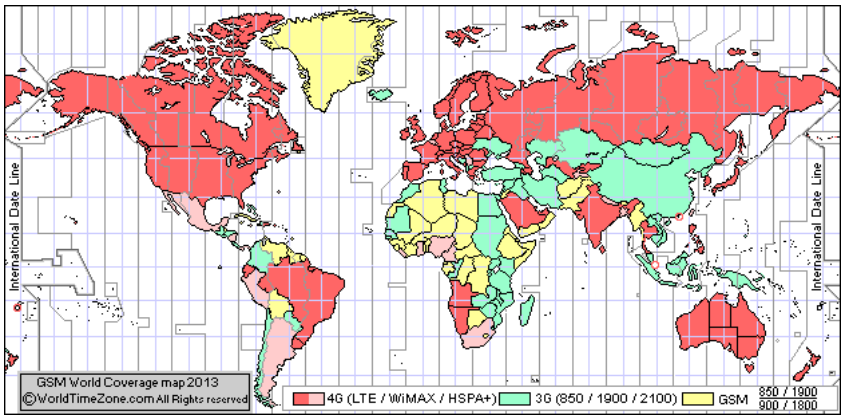
Le numérique est pervasif par définition pourrait-on dire : il est devenu en réseau dans tous ses aspects. Mais lorsqu'il se connecte à d'autres réseaux, transport ou énergie notamment, il finit par redessiner des lignes de coopération, de forces, de faiblesses qui peuvent ne pas recouper des frontières politiques, géographiques ou économiques classiques. C'est une des dimensions de ce que Andrew Barry (2001) a appelé les « zones technologiques » et qu'il a appliqué notamment aux grands oléoducs. Cette approche peut être transposée utilement dans le domaine des infrastructures numériques. Il serait ainsi possible de montrer comment l'Europe a pris de l'avance en matière de téléphonie mobile pendant dix ans sur les Etats-Unis, notamment par la création d'un standard GSM qui unifiait un marché comme zone technologique et qui a permis l'émergence d'un géant des télécoms : Nokia. Mais on a pu voir aussi à quel point les sauts technologiques sont rapides dans ce domaine et comment il devient aisé de rater une marche, en l'occurrence celle des smartphones, pour se retrouver dépassé par d'autres firmes plus innovantes. Le réseau, son harmonisation en standard restent cependant des éléments-clé et les coupures qui ont longtemps existé entre Europe, Asie et Etats-Unis sur ce plan ont depuis été réduites, en partie seulement comme le constate tous les voyageurs qui ne peuvent accéder au réseau du pays où ils arrivent alors qu'ils ne savaient rien des limites des propriétés techniques de leur terminal. La géographie des réseaux et des standards prend dans ces moments-là une matérialité et une importance subjective qui marquent les esprits, habitués à une supposée mondialisation. La carte des standards de communication mobile permet de rendre ces différences encore visibles, même si elle n'a plus le caractère de barrière infranchissable que l'on a pu connaître à l'époque des zones de standards de diffusion des signaux de télévision (avec la grande coupure du monde entre PAL, SECAM et NTSC).

Ainsi l'unification se fait progressivement par domination d'un standard sur un autre (GSM gagnant progressivement sur CDMA toujours actif cependant), bien que des spécificités techniques existent qui peuvent parfois entraîner des difficultés d'usage des terminaux.



Source : http://www.worldtimezone.com

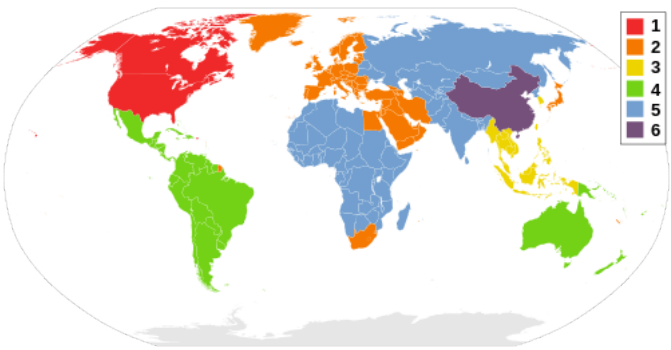
Dès lors qu'on s'intéresse aux standards plus récents et en cours de déploiement, la diversité apparaît encore plus problématique, quand bien même on en reste au même standard (ici le GSM).



Source : http://www.worldtimezone.com

Les données existent aussi pour le standard CDMA par pays et par opérateur mais ne sont pas disponibles sous forme de carte.

D'autres zonages existent pour des raisons purement commerciales (pour empêcher la circulation à des prix trop différents) : c'est le cas des zones DVD, alors que du point de vue technique, une alliance avait été conclue entre les douze constructeurs. Pour pouvoir utiliser un DVD partout dans le monde, il faut le « dézoner », ce qui est illégal et demande une expertise technique élémentaire (les DVD pour PC sont hors zone). Le standard HD qui lui a succédé, le Blu-Ray, a pu tout unifier en écrasant son rival HD-DVD. Ainsi, quantité de frontières hard sont en fait parfois délibérément maintenues ou introduites comme des armes commerciales, politiques, qui sont mises en forme techniques.



Les zones DVD
Source : Wikimedia

Les différences entre pays peuvent aussi porter sur des capacités d'accès, des équipements en terminaux, des tarifs, etc. Nous pourrions alors rejoindre la question de la « fracture numérique » qui nous paraît très mal posée dès lors qu'elle oublie le développement foudroyant des mobiles, mais ce n'est pas l'objet de cet article à vocation principalement géopolitique.

Conclusion

Comme le disait Lawrence Lessig (1999), « *code is law* », ou une autre façon de faire la politique, le code étant la partie la plus *soft* alors que les réseaux, les supports, etc., peuvent en être le *hard* et opérer aussi comme loi, comme producteurs de droit. Il est souvent décidé dans des enceintes qui n'ont rien de démocratiques mais qui relèvent de ce que Ulrich Beck (1997) appelle « *sub-politics* », celle qui se fait dans les laboratoires, les conseils d'administration des grandes firmes et les instances de standardisation par exemple. L'universalité technologique n'a jamais existé, quand bien même nous prétendons vivre désormais dans un monde globalisé. Produire ce supposé « global » demande un travail conséquent et des formats de traduction entre réseaux, standards, protocoles, etc., qui restent différents. Avec Internet, un effort considérable a été réalisé pour faciliter ces traductions. Cependant, cette absence apparente de couture que peut ressentir parfois l'internaute ordinaire, nécessite des accords, des contrôles et des infrastructures matérielles compatibles. La politique de compatibilité est un enjeu de diplomatie technologique majeur. Mais la matérialité des investissements et leur localisation contribuent tout autant à maintenir, à renforcer ou à créer des déséquilibres, des alliances et à donner des leviers de contrôle à certains Etats, à certaines firmes. Ces décisions apparemment techniques sont souvent prises par les firmes elles-mêmes, parfois par les Etats dans des conditions de secret dues à la technicité du domaine mais aussi à son caractère stratégique. Diffuser une connaissance plus large de cette matérialité des réseaux, de la fragilité du monde commun qui s'est construit avec Internet et qui est en train de se cloisonner à nouveau pour toutes les raisons que nous avons évoquées, constitue un enjeu démocratique, pour rééquiper le public en vue d'une forme de contrôle et de participation au débat démocratique sur ces architectures techniques (Boullier 2008, 2012).

Références

• BARRY A. (2001) *Political Machines: Governing a Technological Society*, Londres et New York, Athlone Press.

• BECK U. (1997) *The Reinvention of Politics*, Cambridge, PolityPress.

• BLUM A. (2012) *Tubes. Behind the Scenes at the Internet*, New York, HarperCollins.

• BOULLIER D. (2008) « Politiques plurielles des architectures d'Internet », *Sens Public*, n°7-8, pp. 177-202.

• BOULLIER D. (2012) « Preserving diversity in social networks architectures », in Massit-Follea F., Méadel C. et Monnoyer-Smith L. (dir.), *Normative Experience in Internet Politics*, Paris, Presses de l'Ecole des Mines.

• LESSIG L. (1999) *Code and Other Laws in Cyberspace*, New York, Basic Books.

Le réseau des réseaux serait il devenu, comme le montrent les interceptions massives de la NSA, aisément contrôlable ? Plusieurs propriétés matérielles des tuyaux et des machines qui constituent l'infrastructure d'internet peuvent en effet donner une idée précise des frontières, des filtres et des contrôles possibles : les câbles, les points d'entrée dans les pays, les serveurs de noms de domaine ou des points d'échange internet. La géographie de ces supports techniques essentiels au réseau montre des déséquilibres et des fragilités, que l'on retrouve dans les grands calculateurs ou dans les standards des réseaux mobiles. Mais les arènes politiques manquent toujours pour décider de ces architectures pourtant si cruciales qui formatent notre monde commun, mais pourtant séparé et contrôlé.