# Géopolitique des infrastructures Internet, entre matériel et logiciel

Stéphane Bortzmeyer, Francesca Musiani

# Géopolitique des infrastructures Internet, entre matériel et logiciel

Stéphane Bortzmeyer (Afnic) et Francesca Musiani (CNRS)

PP. 27-43 en Brunessen Bertrand, Guillaume Le Floch (dir.) La souveraineté numérique, Bruylant Editions.

## Introduction. L'infrastructure, quelle importance pour la (géo)politique ?

Dans les débats politiques touchant à l'Internet, l'infrastructure est souvent peu mentionnée. Le débat se focalise sur ce que tout le monde voit, les services. On va donc parler de Facebook, de YouTube, de TikTok, mais bien plus rarement de l'infrastructure qui les porte. Cela peut sembler logique : après tout, on ne fait pas fonctionner l'Internet pour le plaisir de développer une belle infrastructure, on le fait pour permettre l'existence de services. Et ces services sont connus de tou·tes donc semblent un meilleur point d'entrée pour les débats politiques. D'innombrables réunions, rapports, colloques et articles scientifiques ont ainsi été consacrés aux services disponibles sur l'Internet, en se limitant en général à ceux connus du grand public et des médias.

Pourtant, l'infrastructure a une importance dans la (géo)politique. D'abord, évidemment, elle permet le fonctionnement des services. Si les routeurs arrêtent de router les paquets IP, il n'y a plus d'Internet et plus de services. Ceci dit, la plupart du temps, l'Internet marche. Que les mêmes routeurs fassent passer les paquets qui portent le contenu d'un site Web d'extrême-droite, ou ceux qui portent les courriers électroniques d'une association anti-fasciste pourrait faire croire que l'infrastructure est neutre, qu'elle ne joue pas réellement un rôle politique. Mais l'infrastructure a aussi un rôle plus subtil. Certes, il y a des choses qu'elle ne permet pas ou qu'elle empêche. Mais il y a aussi tout ce qu'elle rend plus ou moins facile. L'infrastructure structure, façonne, modèle, permet, empêche ou contraint notre « être-ensemble » sur et avec l'Internet. Si une opération est possible mais que l'infrastructure de l'Internet la rend difficile, réservée à quelques experts, alors, cette opération ne sera, en pratique, pas réellement possible. A priori, on souhaite que les services de l'Internet soient accessibles à tous et toutes.

## Qu'est-ce qu'une infrastructure ?

La notion d' « infrastructure » se réfère typiquement à des systèmes physiques et matériels à large échelle nécessaires pour l'organisation et l'activité humaines, tels que les routes, les ponts, les grilles d'alimentation ou les égouts. Une quantité importante de travaux en géographie, anthropologie et en *science & technology studies* (STS) a désormais été consacrée à explorer les dynamiques de pouvoir, les conflits et contestations, les significations et les rapports sociaux incarnés dans ces infrastructures physiques[1]. Ces travaux définissent, à la base, les infrastructures

[1] Par exemple, HARVEY, P. (2012). "The topological quality of infrastructural relation: An ethnographic approach", *Theory, Culture, and Society*, n° 29, vol. 4-5, pp. 76-92.

comme la matière structurante de nos sociétés, tout en incluant dans l'analyse des infrastructures des aspects a priori immatériels, comme l'information et ses flux (comme on verra ci-dessous). L'analyse des infrastructures permet de penser des agencements à la fois techniques et politiques comme inducteurs, et producteurs, de structures sociales, qui co-façonnent des usages et permettent à des programmes politiques de prendre corps et matière.

Un aspect marquant de la portée analytique de la notion d'infrastructure, ainsi qu'elle est mobilisée par le courant dédié des études sociales des sciences et des techniques (en anglais, *science and technology studies* ou STS), appelé justement *infrastructure studies*, mais aussi dans d'autres disciplines, est le dépassement de l'idée d'une évolution technologique linéaire, inscrite dans la continuité, et de l'idée de progrès des techniques ayant l'efficacité pour pierre angulaire. Les études des infrastructures mettent plutôt en avant les enchaînements de modifications et d'améliorations, et parfois de détournements, propres aux cycles de vie des objets techniques. L'anthropologie des sciences et des techniques place les aspects fonctionnels des infrastructures en arrière-plan, afin d'explorer comment elles sont enchevêtrées dans des ensembles complexes de relations sociales, donnant lieu à des formes infrastructurelles[2]. Il s'agit de réfléchir aux infrastructures en termes d'assemblage socio-économique, qui comporte des liens étroits entre objets techniques et acteurs, qui en sont affectés en retour.

Cette vision s'inscrit dans une réflexion de longue date sur la politique de la matière. Dans *Do Artifacts Have Politics?* (1980) Langdon Winner mettait déjà en avant l'idée « provocatrice » que les technologies possèdent des propriétés politiques, observant à quel point les formes du pouvoir, la justice sociale, l'acte d'exercer ses libertés individuelles et collectives, sont étroitement liés aux structures techniques[3]. La question des infrastructures et de leur relation à l'exercice du pouvoir a permis de proposer une perspective critique sur le développement et l'expansion de systèmes techniques complexes tels que les réseaux de transport ou d'énergie, compris comme substrat, ou support, de la modernité.

La notion d'infrastructure s'est invitée dans les études de l'innovation, porteuse d'interrogations sur la portée « systémique » de grands ensembles techniques et leur relation aux équilibres de pouvoir. Des questions centrales concernent la matérialisation des infrastructures à des niveaux multiples, qui vont du géopolitique au géologique[4], les changements d'échelle[5], ou encore le dévoilement, aux trois niveaux micro-, méso- et macro-, des processus de co-construction idéologique induits par la conception, l'acceptabilité et les utilisations des infrastructures[6]. Un ensemble de travaux ont par ailleurs analysé les usages dans les infrastructures, en montrant comment les effets structurels sont insérés dans une approche plus large, où les usage(r)s contribuent à informer, classifier, catégoriser

---

[2] LATOUR, B., LEMONNIER, P. (eds., 1994). *De la préhistoire aux missiles balistiques. L'intelligence sociale des techniques*, Paris, La Découverte.

[3] WINNER, L. (1980). "Do artifacts have politics?", *Daedalus* 109: 121–136.

[4] EDWARDS, P. (2003). "Infrastructure and modernity: Force, time, and social organization", in T.J. Misa, P. Brey et A. Feenberg (eds.), *The History of Sociotechnical Systems: Modernity and Technology*, Cambridge, The MIT Press, pp. 185-226.

[5] SUBRA, P. (2016). *Géopolitique locale. Territoires, acteurs, conflits*, Paris, Armand Colin.

[6] EDWARDS, op. cit.

et standardiser les infrastructures[7]. Dans ces travaux, l'infrastructure est pensée comme co-produite par les usages, qu'elle contribue à structurer en retour de manière relationnelle, ce qui est censé « re-visibiliser » les infrastructures[8]. Les infrastructures se situent, dans ces perspectives, dans un réseau d'acteurs humains et non-humains qui les conçoivent, les gouvernent et les utilisent, contribuant ainsi à façonner la complexité du social[9]. Il est souhaitable d'être attentifs à la temporalité des infrastructures en plus de leur spatialité, ce qui amène à examiner non seulement le présent des infrastructures, mais « l'anticipation des futurs infrastructurels »[10].

## Infrastructures, usages et « fonctions » politiques

Comme on vient de le voir, une des difficultés des débats sur l'infrastructure est qu'il en existe plusieurs définitions possibles. Concrètement, pour définir ce qu'est une infrastructure dans leur vie quotidienne, certaines personnes vont se limiter à l'infrastructure matérielle, les câbles et les routeurs. À l'inverse, on pourrait utiliser une définition plus large : l'infrastructure, c'est tout ce qui ne se voit pas sur l'écran, mais est indispensable. De ce point de vue, l'infrastructure de l'Internet est analogue à celles qui distribuent l'eau ou l'électricité : tant que tout fonctionne, on ne se rend même pas compte qu'elle existe. Mais nous pourrions aussi adopter une définition un peu différente : l'infrastructure, c'est ce qui permet le fonctionnement du service souhaité, mais que l'utilisateurice ne peut pas facilement changer.

Le mot important est « facilement »: l'utilisateurice peut effectivement changer son résolveur DNS (*Domain Name System*), et c'est souvent fait pour contourner la censure. Mais ce n'est pas une opération triviale pour beaucoup d'utilisateurices, et il est donc raisonnable de compter ce résolveur DNS dans l'infrastructure.

Le fait d'exercer du contrôle sur ces fonctions infrastructurelles fournit à certains acteurs le pouvoir et l'opportunité d'agir à leur avantage. Mais d'autre part, il n'y a que très rarement une seule manière de mettre en œuvre ces fonctions ou un seul et unique acteur capable de les contrôler. Résultat: les infrastructures de l'Internet sont politiques, contestables et contestées, cibles et instruments de gouvernance, objets d'intérêt d'une myriade d'acteurs.

Nous avons dit plus haut que l'infrastructure suscite moins d'intérêt politique que les services. Ce n'est pas tout à fait exact, car la composante matérielle de l'‘infrastructure fait relativement souvent l'objet d'attention, parfois teintée de sensationnalisme, comme dans les récents articles sur le risque de coupure de câbles sous-marins par l'armée russe. En effet, cette composante matérielle semble plus compréhensible, puisqu'elle s'incarne dans des objets tangibles, et qu'elle permet d'illustrer son article avec des photographies. Mais l'infrastructure a aussi une composante logicielle, et on

---

[7] BOWKER, G. C. & STAR, S. L. (1999). *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: The MIT Press; LAMPLAND, M. & STAR, S. L., *Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life*, Ithaca, NY: Cornell University Press, 3–24.

[8] BOWKER, G. C. (1996). "The history of information infrastructures: The case of the international classification of disease", *Information Processing & Management*, vol. 32, n° 1, p. 49-61.

[9] AKRICH, M., LATOUR, B., CALLON, M. (2006). *Sociologie de la traduction : textes fondateurs*, Paris, Presses des Mines ; HARVEY, P., BRUUN JENSEN, C. et MORITA, A. (eds., 2016). *Infrastructures and Social Complexity: A Companion*, New York, Routledge.

[10] BARRY, A. (2020). The material politics of infrastructure. In *TechnoScienceSociety* (pp. 91-109). Springer, Cham.

peut argumenter qu'elle a davantage d'effets sur le vécu de l'utilisateurice. Cette composante plus abstraite est formée des protocoles, des logiciels, et des organisations humaines qui les mettent en œuvre. Nous avons cité par exemple le DNS, exemple typique de cette infrastructure logicielle.

# Infrastructure physique

L'écosystème de technologies qu'on appelle « infrastructures d'Internet » comprend tout d'abord ces artefacts techniques, composantes essentielles d'Internet, dont la fonction infrastructurelle est plus immédiatement évidente : il s'agit des infrastructures physiques de bas niveau, qu'on a pu assimiler aux autoroutes ou aux artères de la société de l'information, et que Susan Leigh Star nous invite « plus sobrement » à apparenter à des « égouts »[11]. Dans l'ensemble, ces infrastructures physiques posent des questions de privatisation et donc de stratégies économiques, de coûts pour l'environnement, de géographies juridiques ; elles soulèvent dès lors des problèmes de gouvernance et de souveraineté qui rejoignent ceux soulevés par la gestion des protocoles, des logiciels d'infrastructure, et des ressources Internet critiques.

## Câbles sous-marins

Ces infrastructures incluent, par exemple, les câbles sous-marins, des milliers et milliers de kilomètres de fibre optique, posés au fond des océans et des mers, liens indispensables entre les réseaux de télécommunication du monde entier. Les enjeux géopolitiques de ces câbles ont une longue histoire[12], et ils posent aujourd'hui des questions telles que le poids des entreprises privées par rapport à celui des États dans leur gestion, le lien de ces infrastructures aux systèmes de surveillance numérique, ou leur impact environnemental à long terme.

## Centres de données

Ou encore, ces infrastructures comprennent les centres de données ou *data centers*, de grands sites physiques sur lesquels se regroupent des équipements constituant un système d'information, notamment des puissants ordinateurs appelés serveurs qui constituent les archives des grandes plateformes[13]. Ces centres de données soulèvent des enjeux tels que la concentration des infrastructures pour un gain économique, de territorialisation du numérique, et du manque de visibilité institutionnelle de ces points de gestion et d'accès à de masses importantes de données[14].

## Internet Exchange Points (IXPs)

Enfin, les *Internet Exchange Points* ou IXPs (dont Laura DeNardis propose une analyse nuancée[15]) sont aussi un exemple de ces infrastructures physiques : il s'agit de grands immeubles hébergeant plusieurs commutateurs de réseau, qui évitent aux opérateurs d'établir des liens directs entre eux, le

---

[11] STAR, S.L. (1999). The ethnography of infrastructure, *American Behavioral Scientist*, 43(3), p. 379

[12] Voir par exemple GRISET, P. (1992). L'Évolution des télécommunications intercontinentales au XXème siècle. *History and Technology, an International Journal*, *8*(3-4), 231-245.

[13] MARQUET, C. (2018). Ce nuage que je ne saurais voir. Promouvoir, contester et réguler les data centers à Plaine Commune. *Tracés. Revue de Sciences humaines*, (35), 75-98.

[14] CARNINO, G., & MARQUET, C. (2018). Les datacenters enfoncent le cloud: enjeux politiques et impacts environnementaux d'internet. *Zilsel*, (1), 19-62.

[15] DeNARDIS, L. (2012b). Governance at the Internet's core: The geopolitics of interconnection and Internet Exchange Points (IXPs) in emerging markets, *Proceedings of TPRC 2012*, en ligne, http://dx.doi.org/10.2139/ssrn.2029715

raccordement au point d'échange permettant à chacun d'échanger du trafic avec tous les autres opérateurs présents. Les IXPs jouent un rôle essentiel notamment dans les marchés numériques émergents, en rapprochant le contenu des utilisateurs, en promouvant la connectivité locale entre les opérateurs régionaux, en réduisant les coûts d'interconnexion et en réduisant la dépendance de la connectivité locale par rapport aux points d'échange étrangers.

# Infrastructure logicielle

Le logiciel d'infrastructure est celui qui ne se traduit pas par un affichage sur l'écran de l'utilisateurice. Absent de l'écran, il est encore moins visible que le matériel. C'est dans cette catégorie que se placent les protocoles qui font tourner le cœur de l'Internet, comme DNS (*Domain Name System*), NTP (*Network Time Protocol*) ou BGP (*Border Gateway Protocol*).

Notez que cette catégorie a des frontières floues. On pourrait y placer les systèmes d'exploitation[16] ou les moteurs de recherche. Selon les critères exposés plus haut, ils ne font pas forcément partie de l'infrastructure, puisqu'on les voit sur l'écran, et que l'utilisateurice les connaît[17]. Et puis on peut les changer, ils ne font pas partie du socle de l'Internet. D'un autre côté, beaucoup d'utilisateurices ne peuvent pas en pratique les changer, soit parce que cela a délibérément été rendu très difficile[18], soit parce que le manque de littératie numérique fait que l'utilisateurice n'imagine même pas être autorisé à changer[19]. Toutefois, à la fois par manque de place, et parce que certains de ces services, comme les moteurs de recherche, ont déjà été largement commentés à la fois dans les médias et dans les articles de recherche, on n'ira pas jusqu'à les traiter ici.

## Les noms de domaine

La partie de l'infrastructure logicielle qui est le plus souvent citée dans les débats politiques de l'Internet est certainement le système des noms de domaine. Les noms de domaine sont ces identificateurs de ressources qui apparaissent dans les adresses de courrier électronique, dans les adresses Web, et dans beaucoup d'autres endroits. Tout le monde a déjà vu des noms comme souvnum.sciencesconf.org ou fr.wikipedia.org. Ces noms sont donc visibles par l'utilisateurice[20] et ne sont pas un simple détail technique, mais également un vecteur de l'identité en ligne. Du fait de leur organisation arborescente, chaque nom est accroché à un nom de niveau supérieur, jusqu'à la racine commune de tous ces noms. Ainsi, souvnum.sciencesconf.org est un sous-domaine de sciencesconf.org qui est lui-même un sous-domaine de org qui est lui-même un sous-domaine de la racine. Cette structure arborescente a joué sur les questions de « gouvernance de l'Internet » un rôle d'aimant, focalisant les discussions. En effet, contrairement à beaucoup d'éléments de l'infrastructure, où on ne distingue pas facilement un centre, une référence sur laquelle la politique pourrait s'exercer, la racine des noms de domaine est un objectif très visible. C'est pour cela qu'elle a fait l'objet de nombreux débats.

---

[16]Dans les débats sur la souveraineté numérique, on a parfois entendu parler de la nécessité d'avoir un « système d'exploitation souverain ».

[17]Au sens où l'utilisateurice en fait un usage délibéré et fréquent au quotidien, ce qui n'empêche pas quelques malentendus. Il n'est pas rare que des utilisateurs, lorsqu'on leur demande le système d'exploitation utilisé, répondent « Google »...

[18]Cas des systèmes d'exploitation des ordiphones, par exemple.

[19]Cas du moteur de recherche, par exemple.

[20]Contrairement à, par exemple, les adresses IP.

## Registres

Chaque domaine qui permet l'enregistrement de sous-domaines est géré par un registre, une organisation qui définit des règles d'enregistrement[21] et qui assure le bon fonctionnement technique des serveurs nécessaires. La régulation de ces registres suscite évidemment des débats politiques et à juste titre puisque, toute présence en ligne nécessitant un nom de domaine, la possibilité d'en avoir un ou pas est cruciale. Comme exemple de règles, on peut noter que .fr est considéré par une loi de 2004[22] comme une ressource nationale, dont le registre est désigné par les pouvoirs publics suite à une procédure comme un appel d'offres public.

## Vie privée

Un autre exemple de politique liée à la gestion des noms de domaine est connu sous le nom de « question whois[23] ». Le titulaire d'un nom de domaine doit donner certaines informations au registre comme son nom, son adresse physique, son numéro de téléphone, etc. C'est déjà un problème de vie privée, puisque certaines utilisations du nom de domaine, même légales, peuvent faire courir des risques au titulaire,qui souhaiterait donc être protégé. Mais il y a plus : pour des raisons opérationnelles (la nécessité de pouvoir contacter quelqu'un en cas de problème impliquant un nom de domaine), ces « données sociales » sont distribuées publiquement. On voit les questions de vie privée que cela peut poser[24]. Pour reprendre un mot de l'ancien directeur de l'ICANN (*Internet Corporation for Assigned Names and Numbers*), « la question whois est notre conflit du Moyen-Orient : très ancienne et sans aucune solution en vue ».

## Gestion de la racine

L'Internet n'a pas de centre, pas de point de contrôle unique. Cela déroute certaines personnes, habituées à des mécanismes politiques hiérarchiques, avec rôles clairs et centralisés. Il y a donc un intérêt important, et à mon avis excessif, porté au rôle de la racine des noms de domaine. Tout domaine est sous-domaine d'un autre et les domaines de premier niveau comme .bf ou .de sont des sous-domaines de la racine, qui peut, en théorie, ajouter ou supprimer des domaines de premier niveau. En pratique, diverses raisons politiques font que cette possibilité de suppression reste purement théorique[25].

## Censure

Quasiment toute activité sur l'Internet passe par l'utilisation des noms de domaine et du DNS. Le DNS est donc à la fois un service critique et un point de contrôle potentiel. Ainsi, en Europe, la technique de censure la plus utilisée est le « résolveur DNS menteur » qui, au lieu de renvoyer

---

[21]Par exemple, pour .fr, il faut avoir une résidence dans l'Union Européenne.

[22]Code des postes et des communications électroniques (2004), Section 2 : Attribution et gestion des noms de domaine de l'internet. (Articles R20-44-34 à R20-44-51), https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070987/LEGISCTA000006165969/2007-02-08/#LEGISCTA000006165969

[23]Du nom du protocole whois d'accès aux informations, même s'il n'est plus depuis longtemps le seul moyen d'accès.

[24]Pour .fr, les données concernant les personnes physiques ne sont pas distribuées, en application de la loi Informatique & Libertés.

[25]Des essais ont été tentés, par des avocats états-uniens contre le .ir de l'Iran au nom de la « lutte contre le terrorisme » ou plus récemment par le gouvernement ukrainien contre le .ru russe. Cf. *ICANN* (2022) Letter to Mykhailo Fedorov, Deputy Prime Minister, Minister of Digital Transformation, Ukraine https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

fidèlement les données obtenues, va les modifier pour empêcher l'utilisateurice d'accéder à un service[26].
Une des conséquences est que certain·es utilisateurices vont alors changer de résolveur (il est habituellement configuré automatiquement), souvent au profit d'une grosse organisation étatsunienne comme Google ou Cloudflare[27].

### Noms de domaine internationalisés

Un autre problème apparemment technique avait suscité de chaudes discussions : les IDN (*Internationalized Domain Names*), des noms qui ne se limitent pas aux caractères utilisés en anglais, comme par exemple réussir-en.fr, 吉电.中国 ou ஆப்பிள்.இந்தியா. Diverses raisons techniques complexes ne permettaient pas de mettre ces noms directement dans le DNS. Il a fallu mettre au point une astuce technique, qui n'a pas été acceptée facilement, beaucoup d'anglophones ne voyant pas l'intérêt de ces noms, et laissant entendre[28] qu'il ne s'agissait pas d'un problème important. L'IETF a fini par normaliser cette technique, que l'ICANN a fini par accepter dans la racine du DNS, après de fortes pressions de gouvernements comme le chinois. La normalisation technique, et l'acceptation par les registres (comme celui de la racine) sont deux étapes importantes mais elles ne suffisent pas, il faut encore que les logiciels acceptent ces noms et les gèrent correctement. Encore aujourd'hui, en 2022, on trouve des cas où ces noms sont incorrectement affichés[29].

## Le routage

Le routage, c'est le système par lequel les messages envoyés sur le réseau, appelés paquets, arrivent à destination. Si un·e utilisateurice situé·e en France veut visiter un site Web chilien, les paquets émis depuis la France (la demande d'une page Web) doivent arriver au bon endroit au Chili, et la réponse (le contenu de la page) doit arriver en France. Le problème serait déjà difficile s'il n'y avait qu'un seul opérateur Internet pour toute la planète. Cependant, l'Internet n'est pas un réseau, mais une interconnexion de réseaux. Il y a plusieurs opérateurs, et il n'existe aucune structure formelle de concertation. Et beaucoup de ces opérateurs sont concurrents.

Le routage nécessite des techniques spécifiques et aussi des coopérations entre humains et entre organisations.

### Les adresses IP

D'abord, le routage nécessite que chaque machine soit identifiée par une adresse unique[30], ce qu'on nomme l'adresse IP (*Internet Protocol*). Un exemple d'adresse IP est celle d'un des serveurs de l'Afnic : 2001:67c:2218:3251::105. Ces adresses IP devant être uniques, il faut un système d'attribution des adresses. Il est fondé sur cinq RIR (*Regional Internet Registry*), chacun responsable d'une zone géographique donnée. Ainsi, l'Europe (au sens large) est sous la responsabilité du RIPE-NCC (Réseaux IPEuropéens – *Network Coordination Center*). Ces RIR

[26]Voir HALL, J., M. AARON, S. ADAMS, B. JONES & N. FEAMSTER (2019). « A Survey of Worldwide Censorship Techniques », https://datatracker.ietf.org/doc/html/draft-hall-censorship-tech
[27]Ces deux entreprises contrôlent les deux plus gros résolveurs DNS publics.
[28]Voire parfois disant ouvertement…
[29]Des raisons de sécurité très contestables sont parfois avancées. En informatique, la sécurité est souvent invoquée pour s'opposer à des changements politiques qu'on n'approuve pas.
[30]Cet article ne peut pas prétendre être un cours complet sur le fonctionnement de l'Internet et sur les protocoles sous-jacents. Cette phrase est donc une simplification. Voir ARTICLE 19 & CATNIP (2021). How the Internet really works, No Starch Press.

attribuent des groupes d'adresses IP, nommés préfixes[31], à des LIR (*Local Internet Registry*) qui sont typiquement des opérateurs réseau. Notez bien qu'il ne s'agit que d'une attribution d'identificateurs. Leur routage effectif dans l'Internet ne dépend pas des RIR mais de décisions décentralisées par les opérateurs[32].

Les RIR, comme les registres de noms de domaine, publient les informations sur les ressources attribuées, et sur leurs titulaires, en utilisant les mêmes techniques (interfaces Web, whois, RDAP).

## Routage dans l'Internet

Pou réaliser une transmission effective des paquets IP de l'origine à la destination, les opérateurs se connectent entre eux. Cette connexion peut être directe (un câble physique entre deux opérateurs) ou indirecte, via un point d'échange (IXP), une structure qui mutualise l'interconnexion entre opérateurs comme, en France, le France-IX. Il n'est évidemment pas possible de connecter chaque opérateur Internet à chaque autre, ils sont trop nombreux et, dans l'exemple plus haut, l'opérateur français n'a peut-être aucune proximité physique avec son homologue chilien. Il y a donc des « opérateurs d'opérateurs » comme Tata, Lumen ou NTT, qui ont une présence mondiale et connectent les opérateurs entre eux[33].

Une fois la connexion physique établie, il faut un accord des deux opérateurs pour échanger du trafic. Cet accord peut se faire de différentes façons, qui ne dépendent que des choix faits par les opérateurs[34] et de leurs rapports de force :

- L'appairage (*peering*), où le pair ne donne accès qu'à son réseau propre. L'appairage réciproque est en général gratuit et souvent sans formalités. On voit aussi parfois des appairages payants, notamment lorsque les deux « pairs » sont de tailles très différentes.

- Le transit, presque toujours payant, où un client achète à un transitaire une connectivité Internet complète.

Par exemple, un petit fournisseur d'accès local va s'appairer à d'autrs acteurs Internet de taille plus ou moins équivalente, et cela gratuitement, mais va se connecter, en payant, à deux ou trois transitaires pour avoir une connexion vers tout l'Internet[35].

Les acteurs de l'Internet qui se connectent échangent ensuite de l'information sur les adresses IP qu'ils savent joindre, avec le protocole BGP (*Border Gateway Protocol*).

---

[31] L'adresse ci-dessus fait partie du préfixe 2001:67c:2218::/47.

[32] Ainsi, en réaction à l'agression russe, le gouvernement ukrainien avait demandé au RIPE-NCC l'annulation des attributions de préfixes IP aux opérateurs russes. Le RIPE-NCC a refusé, en partie parce que cela n'aurait rien changé : les acteurs russes de l'Internet auraient certainement continué à router les préfixes IP même si ceux-ci avaient été officiellement retirés. Cf. *RIPE-NCC* (2022) RIPE NCC Response to Request from Ukrainian Government https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[33] Ceux qui ont réellement une présence partout sont nommés « Tier-1 » mais le terme est souvent galvaudé par le marketing. Et, de toute façon, rappelez-vous bien que ce chapitre est forcément une simplification.

[34] Certains pays, comme la Bolivie, peuvent avoir des lois locales qui encadrent cette interconnexion pour atteindre des objectifs politiques, par exemple pour que le trafic interne au pays ne circule pas via un pays tiers.

[35] Comme l'Internet est une interconnexion de réseaux, vous pouvez considérer le petit réseau local que vous avez à la maison, avec ses deux ordinateurs, sa télévision et ses brosses à dents connectées, comme un réseau dont l'unique transitaire est votre FAI (Fournisseur d'Accès à l'Internet).

## Le chiffrement

Dans le monde numérique, les données peuvent être facilement copiées et traitées ensuite automatiquement, même quand elles sont de très grande taille. C'est bien pour cela que l'informatique a été inventée, et a eu un tel succès. Mais, en sécurité, cette possibilité devient un défaut : un surveillant peut facilement lire le trafic Internet et l'analyser. L'aiguille dans la botte de foin devient facile à trouver. Les révélations d'Edward Snowden ont montré que les États-Unis utilisaient largement cette possibilité, mais ils ne sont évidemment pas les seuls.

La lutte contre cette surveillance massive, et contre d'autres problèmes de sécurité liés à l'absence de protection du trafic IP, passe par différents mécanismes politiques et techniques. Le principal mécanisme technique est le chiffrement. S'appuyant sur la mathématique, il s'agit de faire subir aux données des opérations qui les rendent incompréhensibles pour quelqu'un qui ne dispose pas d'une clé secrète. C'est une technique ancienne mais son utilisation massive en dehors du monde militaire n'est venue qu'avec la généralisation du numérique, qui rend l'espionnage très facile mais permet également le chiffrement généralisé.

Comme souvent en sécurité, le chiffrement ne fait pas que des heureux : ceux qui surveillaient le trafic IP regrettent que le chiffrement les gêne[36]. On voit donc régulièrement des offensives idéologiques contre le chiffrement, puis, plus récemment, pour dire que le chiffrement, « c'est bien, mais… »[37]. Le chiffrement est un bon exemple de controverse politique autour d'une technique d'infrastructure. Le débat mêle des considérations politiques (la légitimité de la surveillance) et techniques (il y a chiffrement et chiffrement ; toutes les façons de chiffrer ne se valent pas[38]).

En général, l'utilisateurice n'est pas conscient de l'existence ou de l'absence de chiffrement. C'est un service qui, pour ielle, est rendu par l'infrastructure et dont la présence ou l'absence n'est pas évidente. L'utilisateurice du Web voit l'utilisation du chiffrement grâce au célèbre « cadenas vert » mais pour les messageries instantanées, c'est moins clair, et le service Telegram a ainsi souvent été pointé du doigt pour le fait qu'il ne chiffre pas systématiquement, mettant ainsi en danger ses utilisateurices.

## La normalisation technique

Plusieurs des points vus ici dépendent d'une normalisation technique, c'est-à-dire de l'établissement de normes écrites, décrivant avec précision ce que doivent faire les logiciels pour que la communication se fasse. La normalisation technique n'est pas, en dépit de son nom, purement technique. Elle a des conséquences directes sur le marché (s'il y a deux solutions techniques, portées par deux entreprises différentes, celle dont la solution accèdera au statut de norme aura un net avantage économique). Et elle a des conséquences pour l'utilisateurice, sur ce qu'ielle pourra faire ou pas ou, plus couramment, sur ce qu'il sera facile de faire ou difficile. C'est par exemple le cas du chiffrement: si la norme technique ne prévoit pas de chiffrement des communications, celui-ci restera possible, mais nécessitera probablement un effort particulier de la part de l'utilisateurice,

[36]Mais ne les empêche pas : comme toute technique de sécurité, le chiffrement n'est pas parfait et ne protège pas contre tout.

[37]ERMOSHINA, K. & MUSIANI, F. (2022). *Concealing for Freedom : The Making of Encryption, Secure Messaging and Digital Liberties*, Manchester, UK, Mattering Press.

[38]Ainsi, si le chiffrement n'est pas « de bout en bout », s'il ne va pas de la machine individuelle de l'émetteur à celle du récepteur, un intermédiaire peut accéder aux données non chiffrées. Les demandes d'affaiblissement du chiffrement sont donc souvent des demandes sur ces intermédiaires.

et d'abord l'effort de comprendre qu'il y a un risque et qu'une action de sa part est nécessaire. En pratique, l'absence du chiffrement dans la norme technique fera que beaucoup d'utilisateurices ne seront pas protégé·es par le chiffrement.

Il est important de comprendre que l'Internet est un réseau « sans permission » : il n'est pas du tout nécessaire qu'une technologie soit normalisée pour qu'elle soit déployée[39]. Des services comme le partage de fichiers avec BitTorrent, ou comme la cryptomonnaie Bitcoin, ont ainsi été largement diffusés sans avoir jamais fait l'objet d'une normalisation. Le Web lui-même a été déployé bien avant de passer par un processus de normalisation.

Il existe plusieurs organisations de normalisation dans l'Internet[40]. On peut par exemple citer l'IEEE (*Institute of Electrical and Electronics Engineers*), qui gère notamment les connexions physiques, ou le W3C (*World-Wide Web Consortium*), connu pour son travail sur les technologies du Web comme HTML ou CSS. Pour le cœur logiciel de l'Internet, le principal organisme de normalisation est l'IETF (*Internet Engineering Task Force*)[41]. L'IETF est une organisation très ouverte[42], qui publie ses normes sous le nom de RFC[43]. Ces RFC sont donc la description technique de comment les protocoles Internet fonctionnent.

Bien que la normalisation ne soit pas obligatoire pour déployer un protocole, elle a quand même une influence : bien des acteurs privilégient les techniques normalisées. Les décisions prises par les organismes de normalisation font donc régulièrement l'objet de controverses, car elles peuvent être néfastes pour certains intérêts. On a vu des exemples avec la version 1.3 du protocole de sécurité TLS (*Transport Layer Security*). Cette version essayait de résoudre des limites de sécurité des versions précédentes mais ceux qui exploitaient ces limites afin de pouvoir observer le trafic malgré le chiffrement ont vigoureusement protesté (ils n'ont finalement pas eu gain de cause). Une autre controverse a éclaté autour du protocole DoH (*DNS over HTTPS*) qui permettait de chiffrer le trafic concernant les noms de domaine, ce qui, vu l'utilisation fréquente du DNS pour la surveillance et pour la censure, a également suscité des polémiques[44]. Enfin, le protocole QUIC[45] a également fait l'objet de débats puisqu'il diminuait cette « visibilité » sur le trafic, visibilité utile aux opérateurs mais également dangereuse pour la vie privée et la neutralité du réseau.

Ce n'est évidemment pas un hasard si ces trois polémiques ont concerné les protocoles de chiffrement ; celui-ci étant l'outil principal de sécurité sur l'Internet, il concentre les critiques.

---

[39]C'est une bonne chose : cela empêche les blocages par les organismes de normalisation et cela retire donc un pouvoir qui pourrait être excessif. Cela encourage l'innovation.

[40]On notera que l'agence de l'ONU, l'UIT (Union Internationale des Télécommunications), ne joue quasiment aucun rôle ici, ce qui explique leur activisme à organiser de nombreuses réunions pour tenter d'exister.

[41]*IETF* (2022) The Tao ; A Novice's Guide to the Internet Engineering Task Force https://www.ietf.org/about/participate/tao/

[42]Au sens où il n'y a pas de barrière formelle à la participation. En revanche, il faut évidemment des compétences techniques, mais aussi du temps et de la patience. Voir *TEN OEVER, N., CATH, C., KÜHLEWIND, M., PERKINS, C.,* RFC 9307, Report from the IAB Workshop on Analyzing IETF Data (AID), septembre 2022 et CATH, C. (2021). Changing Minds and Machines: A Case Study of Human Rights Advocacy in the Internet Engineering Task Force (IETF), PhD thesis.

[43]C'était autrefois le sigle de *Request For Comments* mais il y a bien longtemps que ce n'est plus le cas, même si le sigle est resté.

[44]BORTZMEYER, S. (2022). La prise de décision dans la normalisation technique Internet : l'exemple de DoH, *Terminal*, 132-133, https://journals.openedition.org/terminal/8221

[45]Encore un sigle qui a perdu sa signification originelle, que nous ne citerons donc pas. QUIC est une alternative au principal protocole de transport de l'Internet, TCP.

## Conclusion

Cet article a décrit de nombreuses façons dont les infrastructures de gouvernance d'Internet intègrent dans leurs caractéristiques techniques des préoccupations d'intérêt public, telles que la confidentialité, l'accès au savoir et la liberté d'expression. Comme ces exemples le montrent, les processus de conception et de développement nécessaires pour maintenir Internet opérationnel contribuent, en fin de compte, à la construction de la sphère publique numérique et arbitrent les arrangements de pouvoir, de liberté et d'autorité dans cette sphère. Beaucoup de ces fonctions sont cachées à la vue du public – pas intentionnellement cachées, mais pas nécessairement visibles pour les internautes.

Cet article a montré combien et comment « l'infrastructure compte ». Elle influence, et parfois détermine, ce qu'on va faire ou ne pas faire sur l'Internet. Elle est donc un composant de la souveraineté. Ceci dit, tout ne doit pas être vu à travers le prisme de la souveraineté des États. En effet, presque aucune des fonctions « politiques » que traversent les infrastructures d'Internet, et qui sont décrites dans ce chapitre, n'est principalement gérée par les États et leurs gouvernements, et rarement ces fonctions de gouvernance impliquent une manipulation directe des contenus, ou un engagement direct des individus en ligne. De plus, il n'y a pas de vision nationale sur tous les sujets. Par exemple, quelle serait une « vision française » sur la sécurisation du routage et du protocole BGP ?

Et il faut également éviter de se limiter à la souveraineté des États. Celle-ci s'exerce en effet parfois au détriment des individus. Que devient la souveraineté de l'individu si son fournisseur d'accès à l'Internet contrôle ce qu'il peut faire ou voir ? Par le biais de la notion d'infrastructure, c'est la notion de souveraineté numérique elle-même qui est mise à l'épreuve, en dévoilant une pluralité de « souverainetés numériques » qui sont définies, souhaitées, recherchées, cooptées par les différentes parties prenantes de l'Internet, y compris, bien sûr, les citoyens et citoyennes internautes.

## Références bibliographiques


AKRICH, M., LATOUR, B., CALLON, M. (2006). *Sociologie de la traduction : textes fondateurs*, Paris, Presses des Mines.

ARTICLE 19 & CATNIP (2021). *How the Internet really works*, No Starch Press.

BARRY, A. (2020). « The material politics of infrastructure », in *TechnoScienceSociety,* Springer, Cham, pp. 91-109.

BORTZMEYER, S. (2022). « La prise de décision dans la normalisation technique Internet : l'exemple de DoH », *Terminal*, 132-133, https://journals.openedition.org/terminal/8221

BOWKER, G. C. (1996). "The history of information infrastructures: The case of the international classification of disease", *Information Processing & Management,* 32 (1), p. 49-61.

BOWKER, G. C. & STAR, S. L. (1999). *Sorting Things Out: Classification and Its Consequences,* Cambridge, MA, The MIT Press.

CARNINO, G., & MARQUET, C. (2018). « Les datacenters enfoncent le cloud: enjeux politiques et impacts environnementaux d'internet », *Zilsel*, (1), pp. 19-62

CATH, C. (2021). *Changing Minds and Machines: A Case Study of Human Rights Advocacy in the Internet Engineering Task Force (IETF)*, Thèse de doctorat.

DeNARDIS, L. (2012b). « Governance at the Internet's core: The geopolitics of interconnection and Internet Exchange Points (IXPs) in emerging markets », Proceedings of TPRC 2012, en ligne, http://dx.doi.org/10.2139/ssrn.2029715

EDWARDS, P. (2003). "Infrastructure and modernity: Force, time, and social organization", in T.J. Misa, P. Brey et A. Feenberg (eds.), *The History of Sociotechnical Systems: Modernity and Technology*, Cambridge, The MIT Press, pp. 185-226.

ERMOSHINA, K. & MUSIANI, F. (2022). *Concealing for Freedom : The Making of Encryption, Secure Messaging and Digital Liberties*, Manchester, UK, Mattering Press.

GRISET, P. (1992). « L'Évolution des télécommunications intercontinentales au XXème siècle », *History and Technology, an International Journal*, 8(3-4), pp. 231-245.

HALL, J., M. AARON, S. ADAMS, B. JONES & N. FEAMSTER (2019). « A Survey of Worldwide Censorship Techniques », https://datatracker.ietf.org/doc/html/draft-hall-censorship-tech

HARVEY, P. (2012). "The topological quality of infrastructural relation: An ethnographic approach", *Theory, Culture, and Society*, n° 29, vol. 4-5, pp. 76-92.

HARVEY, P., BRUUN JENSEN, C. et MORITA, A. (eds., 2016). *Infrastructures and Social Complexity: A Companion*, New York, Routledge.

LAMPLAND, M. & STAR, S. L., *Standards and their stories: How quantifying, classifying, and formalizing practices shape everyday life*, Ithaca, NY: Cornell University Press, pp. 3–24.

LATOUR, B., LEMONNIER, P. (eds., 1994). *De la préhistoire aux missiles balistiques. L'intelligence sociale des techniques*, Paris, La Découverte.

MARQUET, C. (2018). « Ce nuage que je ne saurais voir. Promouvoir, contester et réguler les data centers à Plaine Commune ». *Tracés. Revue de Sciences humaines*, (35), 75-98.

STAR , S. L. (1999). « The ethnography of infrastructure », *American Behavioral Scientist*, 43(3)

SUBRA, P. (2016). *Géopolitique locale. Territoires, acteurs, conflits*, Paris, Armand Colin.

WINNER, L. (1980). "Do artifacts have politics?", *Daedalus,* 109, pp. 121–136.