# À propos des coupures des réseaux Internet en Russie

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 2 mars 2022. Dernière mise à jour le 3 mars 2022

https://www.bortzmeyer.org/coupure-russie.html

---

Suite à l'invasion de l'Ukraine par les troupes de Poutine, on a entendu, d'un côté, plusieurs appels à couper d'une manière ou d'une autre les réseaux russes de l'Internet et, d'un autre côté, des annonces comme quoi la Russie allait procéder à de telles coupures. Cet article explore la question uniquement sous l'angle technique (avec toutefois quelques incursions dans la gouvernance de l'Internet). Je ne parle que de l'infrastructure logicielle de l'Internet, laissant de côté les services comme les réseaux sociaux.

D'abord, deux avertissements. Je ne suis pas neutre face à cette guerre, dont la responsabilité revient à 99,9 % à la Russie. Vouloir mettre sur un pied d'égalité l'agresseur et l'agressé (par exemple en refusant de livrer des armes à l'agressé afin qu'il se défende) n'est pas de la neutralité, c'est du soutien à l'agresseur. Il est donc important d'aider <https://kyivindependent.com/opinion/victor-tregubov-are-you-a-foreigner-who-wants-to-help-ukraine-heres-how/> l'Ukraine (et pas seulement via l'aide humanitaire mais aussi directement en aidant l'Ukraine à faire face <https://ukraine.ua/news/donate-to-the-nbu-fund/>). Ensuite, cet article explore les aspects techniques des éventuelles coupures, ce qui ne veut pas dire que je pense qu'elles seraient une bonne idée. (Je vous donne tout de suite mon opinion : non, ce ne serait pas une bonne idée.)

Ah, un troisième avertissement quand même : beaucoup de choses qu'on lit sur les réseaux sociaux au sujet de l'Internet en Russie sont fausses (par exemple lorsqu'on reprend la propagande russe d'un test de déconnexion qui n'a jamais été observé indépendamment). Donc, prudence.

Si vous n'êtes pas familier·e avec la gouvernance de l'Internet, il faudra se rappeler, tout au long de cet article, qu'il n'y a pas de chef ou de président de l'Internet (si dans un article vous tombez sur des phrases comme « l'ICANN, régulateur de l'Internet », vous pouvez arrêter votre lecture tout de suite, elle prouve que l'auteur ne connait pas son sujet). Chaque acteur a son autonomie de décision (dans les limites des lois et de la politique de son pays). Personne n'a, par exemple, l'autorité technique ou politique de couper effectivement toutes les communications avec la Russie, même s'il le voulait.

Commençons par les noms de domaine. On a vu par exemple le gouvernement ukrainien appeler à retirer de la racine <https://eump.org/media/2022/Goran-Marby.pdf> du DNS les TLD russes

.ru, .su et .[Caractère Unicode non montré [1] ][Caractère Unicode non montré ]. Est-ce possible ? Il faut bien discerner la possibilité technique et la possibilité politique. Techniquement, il n'y a guère de difficulté. La copie maitresse de la racine est géré par un sous-traitant du gouvernement étatsunien, Verisign (oui, il y a aussi un rôle de l'ICANN mais, techniquement, ce n'est pas l'ICANN qui édite le fichier de zone de la racine <ftp://rs.internic.net/domain/root.zone.gz>). Il serait techniquement trivial de retirer des TLD de cette zone, comme cela avait été fait pour le .yu <https://www.bortzmeyer.org/fin-de-yu.html>. Cela ne signifierait pas forcément que le .ru et les autres cessent de fonctionner. Le gérant d'un résolveur DNS <https://www.bortzmeyer.org/resolveur-dns.html> peut toujours configurer son logiciel pour transmettre (on parle de "*forwarding*") les requêtes pour les noms sous .ru directement aux serveurs faisant autorité <https://www.bortzmeyer.org/serveur-dns-faisant-autorite.html>. Il est probable que beaucoup de résolveurs en Russie sont déjà configurés ainsi, pour des raisons de souveraineté. Si le .ru était retiré de la racine, d'autres le feraient. On aurait donc une situation compliquée, où le .ru marcherait à certains endroits et pas à d'autres, aggravant la « bordélisation » de l'Internet (qui est déjà assez élevée).

Mais bien sûr la principale question face à cette idée de supprimer les TLD russes est politique : en admettant que l'ICANN et le gouvernement étatsunien décident de le faire (rappelons que même .ir n'a jamais été supprimé, malgré de nombreuses demandes aux États-Unis <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/13/dc-court-rules-that-top-level-domain-not-sub>), cela signifierait la fin immédiate de la racine unique du DNS (RFC 2826 [2]). Les Russes monteraient une autre racine, probablement avec les Chinois, qui seraient ravis du prétexte, et avec d'autres pays qui, jusqu'à présent, supportaient la gestion de la racine par les États-Unis puisque cette gestion restait relativement raisonnable. (Au passage, rappelez-vous que la majorité des informations sur l'Internet dans les médias sont fausses. Il est ainsi inexact de prétendre que Russie ou Chine, avant le 24 février 2022, utilisaient une racine alternative. Des discussions ont eu lieu, des projets ont été montés, mais rien de concret n'a été appliqué.) Comme attendu, l'ICANN a refusé d'agir <https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf>.

Plutôt que de demander la suppression de ces TLD de la racine, une autre solution serait de configurer les résolveurs <https://www.bortzmeyer.org/resolveur-dns.html> pour refuser de résoudre ces noms. Ces résolveurs DNS menteurs sont largement utilisés en Europe pour la censure, par exemple de Sci-Hub. Ils contribuent eux aussi à fragmenter l'Internet. Contrairement aux actions sur la racine, la configuration des résolveurs est très décentralisée : chaque gérant de résolveur peut bloquer .ru de sa propre initiative. En France, ce refus frappe par exemple la chaine RT <https://framagit.org/-/snippets/6522>.

Mais il n'y a pas que le DNS dans la vie. Les techniciens réseau purs et durs diraient même que l'Internet, c'est IP, le DNS n'étant qu'une application, dont on peut se passer. Je ne suis pas vraiment d'accord avec ce point de vue (sans le DNS, on ne va pas très loin), mais cela vaut quand même la peine de regarder ce qu'il en est de la connectivité IP. Sur les listes de discussion RIPE, beaucoup d'intervenants ont réclamé un blocage des adresses IP russes, voire que le RIPE-NCC retire les allocations de préfixes IP et de numéros de systèmes autonomes de la Russie (ou, parfois, seulement du gouvernement russe). (Vu sur le site Web du RIPE-NCC <https://apps.db.ripe.net/db-web-ui/query?searchtext=95.173.136.0%2F24>, un exemple d'un préfixe d'adresses IP alloué à un organisme russe.)

Comme pour le DNS, commençons par ce qui se fait au niveau « central » avant de voir les décisions des acteurs décentralisés. Le RIPE-NCC est le RIR européen et le territoire sous sa responsabilité inclut la Russie (mais aussi l'Iran). Comme l'ICANN, il ne bénéficie d'aucun statut international particulier, c'est juste une organisation de droit néerlandais, qui doit donc obéir aux lois de son pays. C'est

1. Car trop difficile à faire afficher par LaTeX
2. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2826.txt

par exemple le cas lors des sanctions décidées par l'Union Européenne <https://labs.ripe.net/author/athina/how-sanctions-affect-the-ripe-ncc/>. Techniquement, le RIPE-NCC peut en effet modifier sa base de données pour retirer les allocations de ressources russes (pour l'instant, ce n'est pas prévu <https://www.ripe.net/publications/news/announcements/ripe-ncc-executive-board

Toutefois, comme pour le DNS, ce retrait ne se traduirait pas forcément par un effet concret dans les câbles. Chaque opérateur reste maitre de son routage, décide quels préfixes router et quels préfixes bloquer. Certes, beaucoup d'opérateurs filtrent automatiquement les annonces de routage (en général reçues via le protocole BGP) sur la base des bases de données des RIR (ce qu'on nomme l'IRR). Dans l'hypothèse d'une désallocation des ressources russes, ces opérateurs seraient donc coupés de la Russie. C'est d'ailleurs pour cela que Roskomnadzor a demandé aux opérateurs russes <https://twitter.com/LPetiniaud/status/1498272486428921862> (traduction en anglais <https://www.mail-archive.com/frnog@frnog.org/msg69044.html>) de ne plus utiliser comme IRR celui du RIPE-NCC. Mais d'autres opérateurs n'appliquent pas aveuglément les IRR, surtout si ceux-ci étaient trop clairement utilisés pour mettre en œuvre des décisions géopolitiques. Il n'est donc pas du tout sûr que le routage soit coupé, seulement pertubé (encore un cas de « bordélisation » de l'Internet).

Notez bien que les adresses IP éventuellement désallouées ne pourraient pas être réaffectées à d'autres : comme les anciens titulaires russes continueraient certainement à les utiliser, ces adresses ne fonctionneraient pas réellement aux mains de leurs nouveaux titulaires, en raison des nombreux conflits que cela générerait.

L'effet d'une désallocation serait plus fort si le routage était uniformément sécurisé via la RPKI. Mais ce n'est pas partout le cas.

Là encore, la principale conséquence néfaste pour l'Internet viendrait de la fin du système actuel de gestion des ressources : au lieu de RIR internationaux, on verrait différents pays monter des registres concurrents, des adresses être attribuées deux fois et autres désordres.

Là aussi, comme pour le DNS, il peut y avoir des décisions locales. Un opérateur peut refuser les paquets IP venant d'adresses russes ou bien refuser les annonces BGP contenant des AS russes. On verra sans doute dans les prochaines semaines un paysage compliqué, où certaines communications marcheront à certains endroits.

Jusqu'à présent, j'ai parlé de la possibilité que des gens à l'extérieur de la Russie coupent les communications avec la Russie. Mais la coupure peut aussi se faire suite à une initiative russe, par exemple pour empêcher les citoyens russes de s'informer librement. Pour l'instant, cela ne semble pas être le cas <https://framagit.org/-/snippets/6520> (et on peut regarder RT <https://puck.nether.net/pipermail/outages/2022-March/014284.html>).

Enfin, le texte du gouvernement ukrainien qui appelait à couper `.ru` mentionnait également les AC. Elles ne dépendent pas de l'ICANN ou des RIR, et prennent leurs décisions de leur côté, selon les lois du pays dont elles dépendent. Si elles décidaient de révoquer les certificats russes, on se retrouverait avec des problèmes analogues : une communication partielle, la Russie qui monterait ses propres AC, et, d'une manière générale, un affaiblissement de la sécurité.