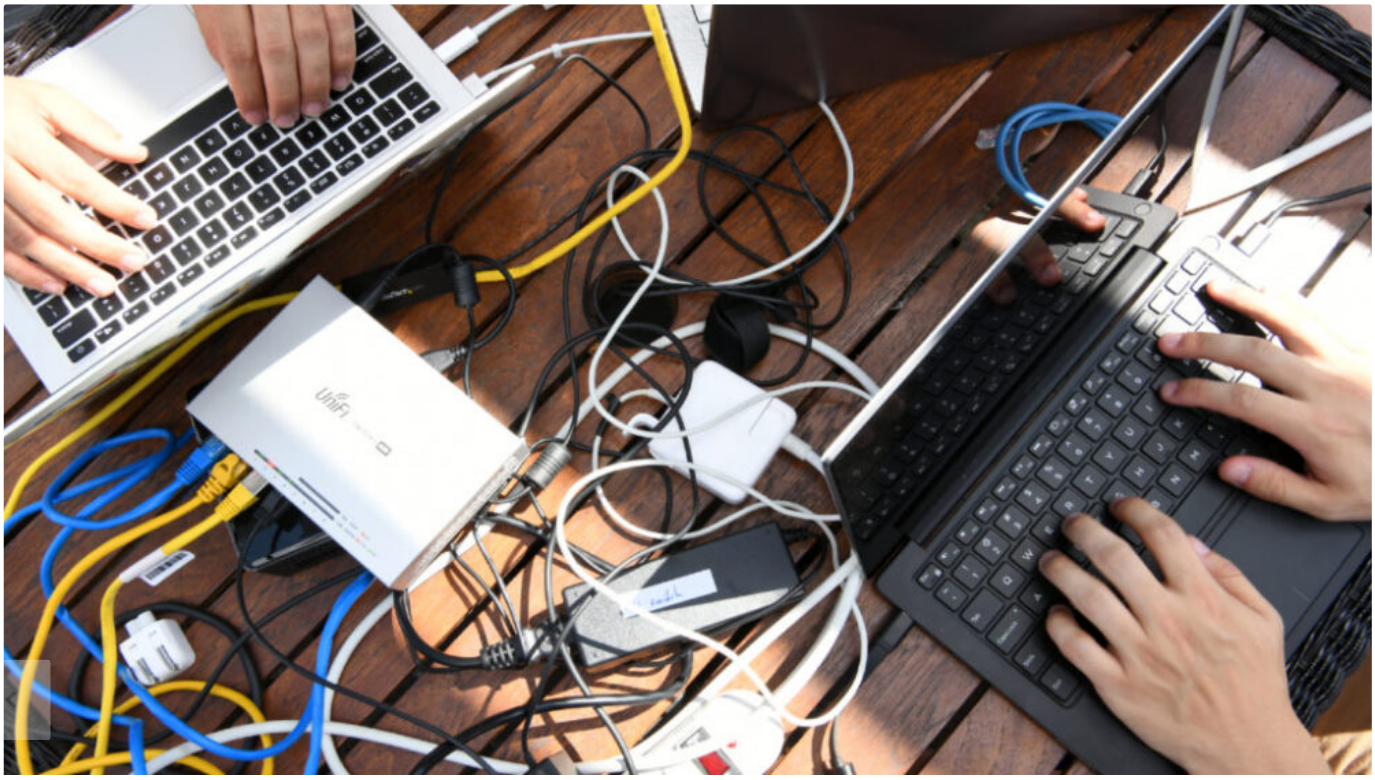
LE RUBICON

La Russie peut-elle se déconnecter d'Internet ?

Kevin Limonier | 24 mars 2022 | ARTICLES |



En 2019, la Douma a adopté la loi FZ90, baptisée loi du « Runet souverain ». Elle prévoit de donner à l'Etat les moyens juridiques, administratifs et techniques de contrôler l'intégralité des flux de données entrant et sortant du territoire russe et, le cas échéant, de déconnecter le pays du reste du monde en cas de « menace extérieure avérée ». Plusieurs semaines après le début de l'invasion de l'Ukraine par la Russie, la déconnexion prévue par la loi de 2019 n'a toujours pas eu lieu, alors même que le pays est progressivement isolé de nombreux flux financiers, logistiques et économiques de la mondialisation soit par des sanctions, soit par l'action du gouvernement russe lui-même.

Cela ne signifie pas pour autant qu'il ne se passe rien dans le cyberespace russophone : le blocage des derniers médias indépendants du pays, de même que celui de plusieurs sites d'information occidentaux, est déjà une mesure de déconnexion de la Russie de certains flux d'informations considérés comme « indésirables » par les autorités en raison de leur couverture de l'invasion russe. De même, l'Etat a demandé à Roskomnadzor, le gendarme russe des télécommunications, de ralentir ou de bloquer certains réseaux sociaux tels que Facebook, au prétexte que ceux-ci seraient des vecteurs de « fausses informations » sur le conflit.

Catastrophiques en termes de liberté d'expression et d'information, ces mesures constituent la suite logique des politiques de censure progressivement établies par les autorités depuis de nombreuses années. Il n'y a pourtant là aucune innovation majeure, mais plutôt une accélération spectaculaire du long mouvement qui vise à déconnecter l'espace informationnel russe de celui des pays occidentaux. D'ailleurs, et même si cela reste anecdotique à l'échelle de l'ensemble la population russe, des solutions de contournement de cette censure numérique existent : la massification des VPN, ou l'utilisation du réseau TOR, conseillée par exemple par la BBC à ses lecteurs situés en Russie où le média est bloqué, permet pour l'instant de dépasser bien des restrictions – du moins pour celles et ceux qui disposent des connaissances techniques nécessaires.

Ces éléments de censures sont pourtant bien loin de la fameuse déconnexion voulue par la loi de 2019. Car si elle venait à survenir, aucun VPN ni aucune ruse numérique ne suffirait à contourner un tel blocage. Les flux de données seraient interrompus

ou filtrés à des niveaux qui laisseraient peu de marge de manœuvre au contournement d'un tel « rideau de fer » numérique. Cet article a pour objectif d'exposer les origines, principes, perspectives et surtout limites de la stratégie portée par la loi de 2019 de « frontiérisation » de l'Internet russe. En effet, la Russie semble ne pas (encore) être capable d'opérer une telle déconnexion, notamment pour des raisons structurelles qui ont trait à l'histoire et à la géographie du pays, de même qu'à l'architecture particulière de son réseau Internet.

Le Runet et ses « frontières numériques » : une construction géopolitique

La loi de 2019 et l'ambition qu'elle porte sont le résultat d'un lent phénomène de prise de contrôle de l'Internet russophone, le Runet, par le pouvoir ou par des intérêts proches de lui. Cette dynamique commence au début des années 2010. Nous sommes alors au lendemain des Printemps arabes, lors desquels les mobilisations en ligne jouèrent un rôle important. A l'hiver 2011-2012, la Russie est elle-même touchée par une vague de manifestations partout dans le pays pour protester contre l'intention de Vladimir Poutine de briguer un troisième mandat présidentiel. Ces mobilisations, dont l'ampleur est inédite depuis la chute de l'URSS, sont largement organisées sur les réseaux sociaux – un type de plateformes alors relativement nouveau, et que les services de sécurité maîtrisent mal.

Après son retour au Kremlin en mars 2012, Vladimir Poutine entame une politique beaucoup plus autoritaire connue sous le nom de « tournant conservateur ». Internet, qui était jusque-là regardé avec une certaine indifférence par les autorités, est désormais considéré comme une menace pour la stabilité du régime. Quelques mois plus tard, les révélations de Snowden ont fourni au pouvoir russe le prétexte idéal pour prendre les dispositions qui s'imposaient afin, comme le titrait alors la Voix de la Russie, « d'échapper aux grandes oreilles de l'Oncle Sam » et de soustraire la population russe au « relativisme moral » dont on disait à Moscou qu'il menaçait de provoquer une révolution de couleur en Russie.

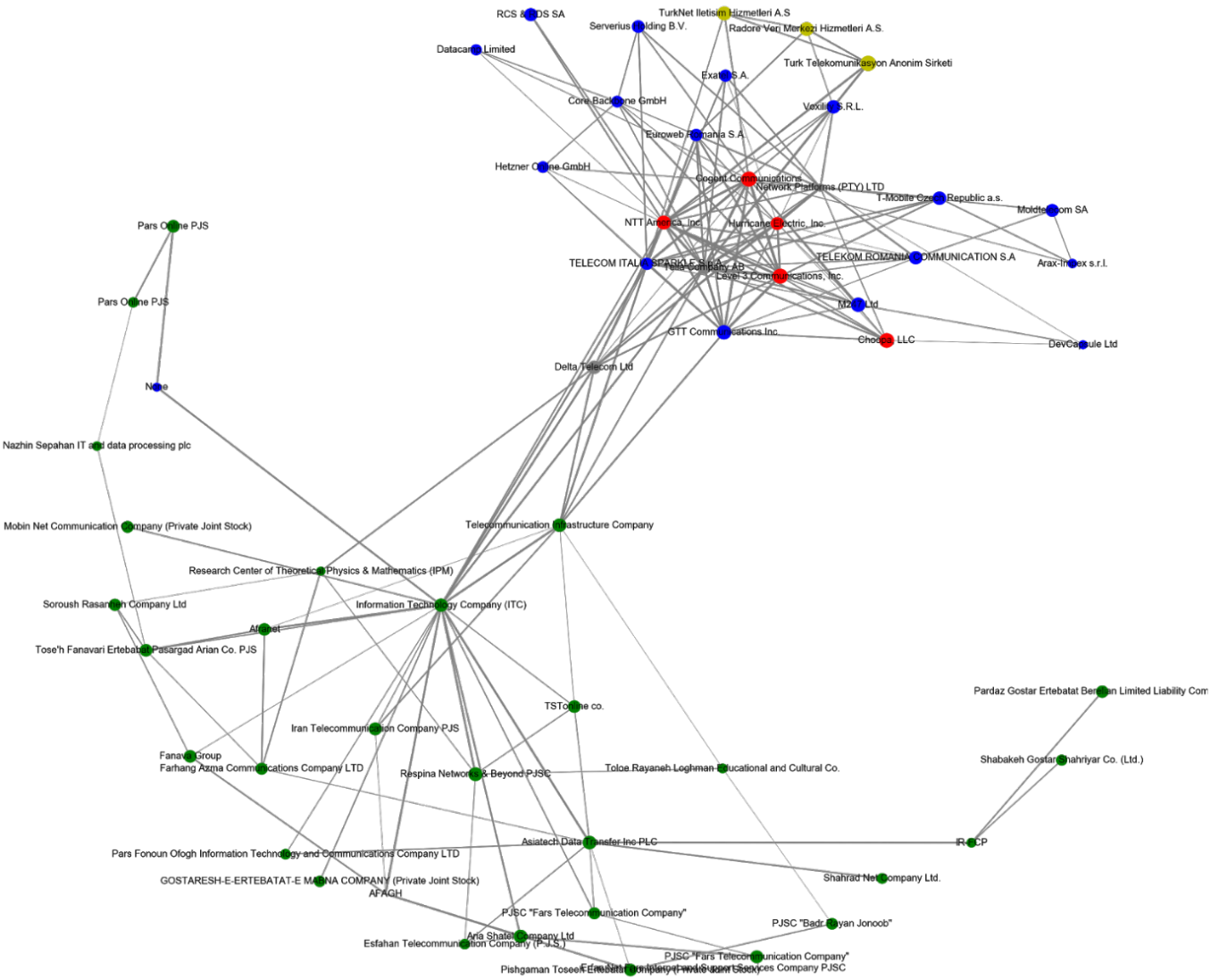
Entre dénonciation de l'hégémon numérique américain, défense des valeurs morales et impératifs de sécurité nationale, Internet devint alors en Russie l'objet d'une triple convergence conduisant à une intense production législative toujours en cours au début des années 2020, et dont la loi de 2019 est le dernier avatar. Il s'agit là d'un lent phénomène d'intégration du Runet à l'univers géographique, mental, stratégique et culturel du pouvoir russe et de ses représentations du monde. Internet, que V. Poutine qualifia un jour « d'invention de la CIA », a longtemps été perçu comme un vecteur d'influences occidentales dangereuses. Progressivement, le terme Runet, qui désignait jusqu'alors le segment de l'Internet où l'on utilise la langue russe pour communiquer, fut récupéré par les autorités qui en fit la projection numérique de ses ambitions géopolitiques : recréation d'une sphère d'influence régionale, instrumentalisation de la pratique de la langue russe, dénonciation de l'hégémonie morale de l'Occident … etc.

Les « frontières numériques », un objet technique

Ce Runet avait donc besoin de frontières (mentales, culturelles, politiques et techniques) pour exister en tant qu'objet cohérent avec la geste géopolitique du Kremlin, et pour proposer une alternative au modèle de l'Internet global, ouvert, et perçu comme dangereux. C'est précisément l'objet de la loi de 2019, qui entend instituer de véritables « postes frontières numériques » permettant de contrôler, ou de bloquer, le trafic entrant et sortant du pays. Pour ce que l'on en sait, l'implémentation technique de cette loi repose sur la capacité de l'État à réorganiser en profondeur les logiques de routage qui structurent l'Internet, notamment grâce à des « appareils de lutte contre les menaces » (TSPU) que les opérateurs et les FAI ont désormais l'obligation d'installer sur les points nodaux de leur réseau. Se présentant sous la forme de boîtiers exploités par Roskomnadzor, le gendarme russe des télécommunications, les TSPU ont un objectif double : d'une part, permettre à l'État russe de pratiquer ce droit de regard conféré par la loi de 2019 sur les paquets de données qui entrent et sortent du territoire ; d'autre part, exécuter l'ordre de déconnexion du segment russe de l'Internet en cas de menace extérieure.

Pour ce faire, les TSPU doivent agir principalement sur la couche BGP de l'Internet. BGP est le protocole qui permet aux sous-systèmes qui composent l'Internet de communiquer entre eux. Ces sous-systèmes, qui sont appelés systèmes autonomes (AS), sont les briques élémentaires de l'Internet. Concrètement, un AS correspond à un fournisseur d'accès Internet, un opérateur de câble, une administration… bref, une entité ayant une gestion autonome de son propre périmètre. Pour que deux AS puissent échanger entre eux des données, il faut qu'ils aient contracté un « accord BGP » (*BGP agreement*) – c'est-à-dire une entente, contractuelle ou non, qui régit les modalités selon lesquelles deux systèmes autonomes vont échanger entre eux des données. Or, aucun AS n'entretient d'accord BGP avec la totalité des autres AS qui constituent l'Internet, dans la mesure où ces accords sont le produit de relations contractuelles entre les gestionnaires de réseaux, et sont donc le fruit de négociations commerciales, techniques, qui peuvent être influencées par des considérations politiques ou même géographiques. La principale conséquence de ce constat est que, pour parvenir d'un point A à un point B de l'Internet, un paquet de données envoyé par un utilisateur à un autre passera généralement par plusieurs AS intermédiaires, dessinant ainsi un chemin logique. Par ailleurs, si tous les AS du monde ne sont pas interconnectés entre eux, alors cela veut dire qu'il y en a qui sont plus centraux que d'autres. Dans certains

pays tels que l'Iran, certains AS font même office d'interface entre réseau national et le reste du monde – créant des goulots d'étranglement stratégiques qui sont contrôlés par les autorités ou des intérêts proches de celles-ci.

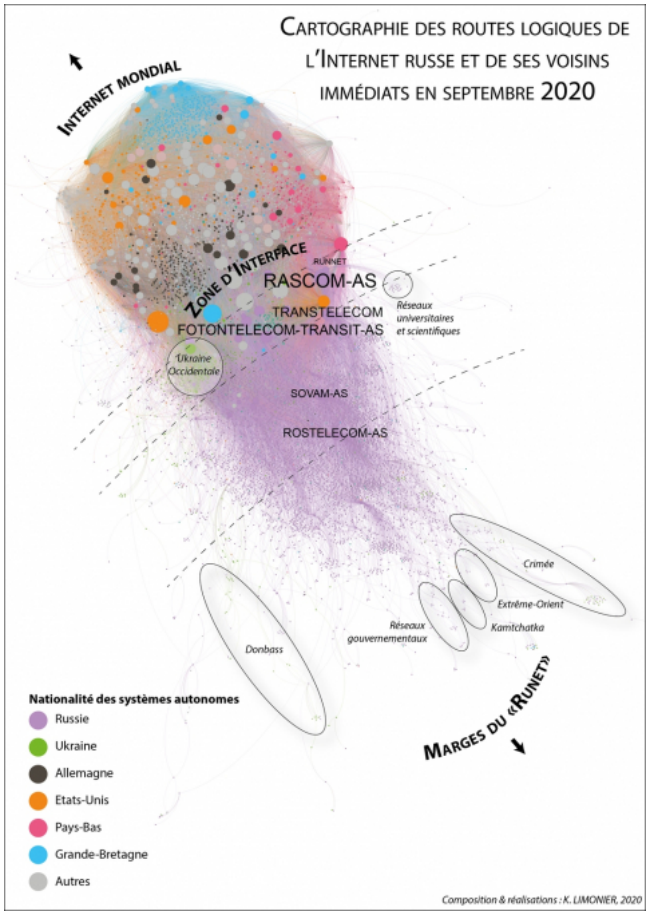


Graphe indiquant la totalité des AS iraniens (en vert) et leurs voisins étrangers, c'est-à-dire les AS non-iraniens faisant l'interface avec le reste de l'Internet mondial. On remarque d'emblée qu'il n'existe que quelques points de passage entre l'Iran et le reste du monde.

C'est justement sur ces goulots d'étranglement que les autorités russes espèrent pouvoir filtrer, voire couper, les flux de données entrant et sortants du territoire fédéral – notamment grâce aux boitiers TSPU. Sur le papier, il suffirait donc aux autorités de décréter une déconnexion pour qu'elle ait lieu via ces infrastructures. Or, la plupart des tests qui ont été menés par le gouvernement ne semblent pas avoir eu les effets escomptés : ils ont même été reportés *sine die*, officiellement en raison de la crise sanitaire. Depuis, l'activité est restée très faible sur ce front, y compris depuis le début de l'invasion de l'Ukraine.

Le Runet, l'un des réseaux les plus complexes du monde

La Russie semble donc connaître d'importantes difficultés pour implémenter sa loi sur le « Runet souverain ». L'hypothèse ici formulée est que ces difficultés sont d'abord dues à la structure même du réseau russe, qui est l'un des plus complexes du monde : il comporte trop d'acteurs, trop de portes d'entrée, trop de chemins de traverse. Bref, il est aux antipodes des réseaux chinois ou iraniens qui, organisés autour de quelques points de passages centralisés, sont facilement contrôlables et regardés à Moscou comme des exemples à suivre.



Le graphe ci-dessus montre l'ensemble des systèmes autonomes russes et leurs voisins, c'est-à-dire des systèmes autonomes étrangers permettant à la Russie de se connecter au reste du monde. La différence avec le réseau iranien est flagrante : le nombre de routes et d'AS connectant la Russie au reste du monde est sans commune mesure avec les quelques points soigneusement établis par Téhéran pour contrôler son réseau.

En fait, la Russie a l'un des réseaux les plus complexes et les plus denses du monde. En décembre 2020, 6575 systèmes autonomes déclaraient être enregistrés en Russie selon le RIPE. Ce chiffre place la Russie en troisième position dans le classement des pays disposant du plus grand nombre d'AS, derrière les États-Unis (28914 AS) et le Brésil (8566 AS), mais loin devant l'Allemagne (3034 AS) ou la France (2111 AS). Outre le foisonnement d'acteurs, le nombre de routes BGP qui charpentent l'Internet russe est également considérable. Selon nos données, il existe au moins 12 582 accords BGP à l'intérieur des frontières russes. C'est trois fois moins que les États-Unis (37000 accords), mais deux fois plus que l'Allemagne (6269 accords) et dix fois plus que la France (1165). Cela signifie que pour atteindre n'importe quel point de l'Internet russe, le nombre de routes qu'un paquet de données peut emprunter est considérable, difficilement cartographiable, et donc difficilement contrôlable.

Cette situation s'explique en grande partie par l'histoire : au début des années 1990, l'Internet mondial ressemblait beaucoup à l'Internet russe contemporain, avec une foule de petits AS connectés les uns aux autres. Mais l'explosion du nombre d'internautes dans le monde occidental à partir du milieu des années 1990 a fait émerger de grands acteurs et disparaître quantité de petits. En Russie, un tel mouvement n'a pas eu lieu avec la même intensité, en raison du manque d'investissements, notamment publics, pour développer une connectivité rapide sur l'ensemble du territoire. Outre le manque de moyens, la taille du territoire a également été un facteur important : de nombreuses villes éloignées des grands axes de communication n'intéressaient pas les quelques grands opérateurs russes, car trop chères à connecter pour si peu d'abonnés potentiels. De fait, une foule d'initiatives « par le bas » sont venues pallier ces difficultés – donnant naissance à une quantité de petits opérateurs aujourd'hui bien implantés.

Résistance passive de la part de certains opérateurs

Ce foisonnement de routes et d'acteurs limite *a priori* l'efficacité de la stratégie du Runet souverain, que ce soit pour le filtrage du réseau ou pour procéder à sa déconnexion en cas de menaces extérieures. Si l'on regarde ce qui se passe dans des pays qui parviennent aujourd'hui à contrôler efficacement leur réseau, tels que la Chine ou l'Iran, on s'aperçoit qu'ils ne possèdent qu'un petit nombre de routes internationales, détenues par des acteurs contrôlés par l'État ou proches de ses intérêts. Dès lors, on peut postuler que l'un des objectifs des autorités russes est de réduire ce nombre de routes et de composer des corridors logiques maîtrisés, d'abord grâce à un recensement des routes, puis ensuite en demandant aux AS d'en supprimer certaines. Un

centre de monitoring du réseau a même été mis en place récemment, afin de coordonner l'action des autorités avec celle des systèmes autonomes et des opérateurs, non sans rencontrer d'importantes difficultés qui témoignent possiblement du manque de coopération des milliers de FAI que compte le pays avec les autorités – voire même d'une certaine forme de « résistance passive » vis-à-vis de l'État russe.

Cette défiance provient essentiellement d'un profond manque de confiance des opérateurs vis-à-vis des autorités. Selon la loi, chacun des opérateurs disposant de ses propres infrastructures et de son propre système autonome a l'obligation d'installer sur ses routeurs un appareil TSPU, afin de filtrer ou de bloquer le trafic sur ordre des autorités. Pour installer ces appareils, les opérateurs doivent par exemple aménager à Roskomnadzor un accès à tous les routeurs qu'ils administrent, mais aussi, et surtout lui communiquer la structure interne de leurs réseaux. Or, ainsi que le faisait remarquer fin mars 2021 un haut-responsable de FAI sous couvert d'anonymat, « *où est la garantie qu'un jeune collaborateur* [de Roskomnadzor], *avec son tout petit salaire, ne décide pas demain de revendre ces données* [au marché noir] ? ». Dans un pays toujours confronté à de graves problèmes de corruption, la question est importante. De nombreux jeux de données récoltées sur demande des autorités sont en effet régulièrement revendus au marché noir, et celles concernant la structure interne du réseau d'un opérateur peuvent se revendre très cher, car elles peuvent faciliter certaines cyberattaques.

Le flou juridique qui entoure le déploiement des TSPU encourage d'ailleurs cette méfiance. Par exemple, si la loi précise bien que l'appareil est aux frais de l'État, elle est muette sur le fait de savoir qui doit en payer l'entretien, ainsi que les frais annexes engendrés par l'installation. Ainsi, la loi exige par exemple que le TSPU soit situé dans un local sécurisé, auquel même l'opérateur ne peut avoir accès. Pour un petit opérateur municipal, il s'agit d'un surcoût considérable et, compte tenu du manque de confiance envers les autorités, aucune illusion n'existe sur une possible prise en charge des frais par l'État. Plus largement, une véritable défiance s'est installée vis-à-vis des autorités, tandis que les opérateurs sont depuis longtemps rompus à la pratique d'une certaine "résistance passive" vis-à-vis des injonctions de surveillance numérique du pouvoir.

Déconnecter la Russie du reste de l'Internet : un objectif encore lointain ?

Est-ce à dire que l'objectif de déconnexion contrôlée voulu par la loi de 2019 reste encore inatteignable ? La question reste bien évidemment en suspens. Depuis le début de l'invasion de l'Ukraine par la Russie, les manifestations de l'autoritarisme poutinien ont connu une intensification sans commune mesure, qui pourraient bien réduire à néant les tactiques d'évitement des opérateurs réticents. En parallèle, les boitiers TSPU semblent au moins en partie opérationnels puisque c'est grâce à eux que certains réseaux sociaux occidentaux sont actuellement ralentis en Russie. Dès lors s'opère une déconnexion progressive des ressources informationnelles non contrôlées par le pouvoir russe, qui s'avère bien plus pernicieuse qu'une rupture totale et brutale avec le reste du réseau.

Car même si la déconnexion s'avérait possible à l'heure actuelle, rien ne permet d'affirmer que le Runet pourrait continuer de fonctionner une fois la déconnexion effectuée. Trop de ressources se trouvent hébergées à l'étranger, sans parler des serveurs DNS qui, même s'ils se situent dans la zone .ru, peuvent renvoyer à des infrastructures localisées hors de Russie. Certes, le problème est connu et sérieusement pris en considération, comme le montre une récente circulaire interne du Ministère des télécommunications (qui a pu être considérée à tort comme le signe avant-coureur d'une déconnexion du pays), qui demande aux administrateurs de sites publics russes de rapatrier sur le territoire fédéral la totalité de leurs ressources. Mais pour le reste des ressources Internet, l'État russe est encore impuissant à leur imposer de telles directives, et le Runet demeure encore beaucoup trop dépendant de ressources extérieures à la Fédération pour qu'une déconnexion du pays ait lieu sans faire disparaître la moitié du réseau russe.

Pour autant, certaines mesures prises par des acteurs occidentaux pourraient bien aider la Russie à parvenir à son objectif de contrôle total de ses frontières numériques. C'est notamment le cas lorsque certains opérateurs occidentaux de transit tels que Cogent décident de ne plus desservir la Russie. Il en résulte une diminution du nombre de routes internationales permettant de connecter le pays au reste du monde, augmentant par là sa capacité de contrôle sur les chemins restants. Sans compter que de telles mesures accroissent la dépendance de la Russie aux ressources chinoises.

Cet article est une adaptation mise à jour de la publication académique suivante : Kevin Limonier, « Vers un « Runet souverain » ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », EchoGéo [en ligne], 56.

Credit : U.S. Air Force (R.J. Biermann)

•— ••— — • ••— •—• •••

Kevin Limonier

Kevin Limonier (@kevinlimonier) est géographe, maître de conférences à l'Institut français de géopolitique (Université Paris 8) et directeur adjoint du centre GEODE. Il est spécialiste du cyberespace russophone et plus largement de la cartographie géopolitique des réseaux numériques.

Comment citer cette publication

Kevin Limonier, « La Russie peut-elle se déconnecter d'Internet ? », *Le Rubicon*, vol. 2, 24 mars 2022 [https://lerubicon.org/la-russie-peut-elle-se-deconnecter-dinternet/].