Cas d'utilisation du Mode de fonctionnement du réseau Internet

Interconnexion et routage

Septembre 2020

Effets des politiques en matière de réglementation du routage et de l'interconnexion, ainsi que de la réduction de l'autonomie des opérateurs sur le Mode de fonctionnement du réseau Internet

Dans un certain nombre de pays, la réglementation tend à contrôler davantage la façon dont les opérateurs d'Internet gèrent l'interconnexion et le routage du réseau. Les choix en matière d'interconnexion et de routage sont des décisions cruciales, prises pour des raisons locales et opérationnelles afin d'assurer la résilience du réseau et l'optimisation des flux de trafic. Dans ce cas d'utilisation, nous nous intéresserons à différentes facettes de cette tendance dans trois pays, la Chine, la Russie et les États-Unis, où la réduction de l'autonomie des réseaux en matière d'interconnexion et de routage nuit à deux propriétés essentielles du Mode de fonctionnement du réseau Internet :

- Une infrastructure ouverte et accessible dotée d'un protocole commun
- Une gestion décentralisée et un routage distribué

Plus le fonctionnement d'Internet applique ces deux propriétés essentielles, plus il offre d'ouverture et d'agilité pour les innovations futures et plus les bénéfices sont élevés en matière de collaboration, de résilience, de portée mondiale et de développement économique. Moins Internet applique le Mode de fonctionnement du réseau Internet, moins il ressemble au réseau mondial qu'il devrait être, avec tous ses avantages.

Les nombreuses critiques portant sur le faible nombre de goulets d'étranglement du réseau en Chine ou sur la législation relative à l'« Internet souverain » en Russie ont attiré l'attention sur leurs effets politiques, sociaux ou économiques. En août 2020, le programme « Clean Network » proposé par le gouvernement américain a également donné lieu à des inquiétudes au sein de la communauté technique quant à son inadéquation à ses objectifs cibles et aux dégâts qu'il pourrait entraîner sur l'architecture ouverte qui sous-tend le Mode de fonctionnement du réseau Internet. Ce cas d'utilisation utilise les propriétés essentielles du Mode de fonctionnement du réseau Internet pour apporter une perspective supplémentaire sur la façon dont ces évolutions affectent l'infrastructure d'Internet, et amène à réfléchir aux effets que pourraient avoir ces lois et politiques sur Internet si elles restaient en vigueur ou se généralisaient.

La topologie déformée et hiérarchisée du réseau chinois a un impact massif sur sa portée mondiale et limite l'interconnexion collaborative des réseaux. En Russie, la lourdeur du système de déclaration et la tendance actuelle à la centralisation du contrôle amenuisent de façon drastique l'autonomie et l'agilité des fournisseurs d'accès à Internet, ce qui rend les réseaux moins résilients à une époque où cette résilience est précisément ce dont ils ont besoin. Certaines des exigences du programme Clean Network américain nuisent à l'interconnexion des réseaux, au

développement de l'infrastructure de communication d'Internet, et, par conséquent, aux services et possibilités qu'offre celui-ci.

Tandis que la topologie du réseau chinois ne lui ressemble que de loin sur le plan de ses propriétés essentielles, Internet demeure reconnaissable dans les réseaux russes. Cependant, si de nouvelles mesures visant à centraliser le processus décisionnel et le routage étaient mises en place afin de faire correspondre les réseaux russes aux frontières nationales, le pays risquerait de perdre sa place au sein de l'Internet mondial, en suivant le modèle « d'intranet » national chinois. Les limites que le programme Clean Network envisage d'imposer à l'interconnexion augmenteront le risque de fragmentation d'Internet, donnant ainsi naissance à un Internet fragmenté, un « splinternet ».

Interconnexion et routage en Russie

En Russie, Internet est assez dynamique, avec de nombreuses interconnexions régionales et internationales et plus de cinq mille réseaux en fonctionnement dans le pays.[1] Près du tiers de ces réseaux sont des registres Internet locaux, ce qui signifie qu'ils obtiennent leur espace d'adressage directement auprès du RIPE NCC, le registre Internet régional européen. L'espace d'adressage n'étant pas assigné à ces réseaux par leur fournisseur en amont, ils peuvent changer plus facilement de fournisseur de transit et disposent en général d'une plus grande autonomie quant à leurs choix de connexion que des réseaux de dimensions comparables en Chine.

Cependant, la loi sur l' « Internet souverain » de 2019,[2] qui vise à répondre aux menaces étrangères perçues sur le réseau national, donne aux organismes de réglementation la possibilité de couper la connectivité internationale ou des services (notamment les services de cloud) dont l'Internet russe a besoin. Les opérateurs de réseau devront fournir à Roskomnadzor, l'organisme de réglementation[3], les plans des réseaux, les caractéristiques techniques des équipements de communication où des « mesures techniques pour contrer les menaces » (Technical Means of Countering Threats, TMCT) seront mises en place et des informations sur les canaux de communication (nombre, propriétés physiques, débit, charge moyenne et maximale) et les lieux des installations prévues de TMCT.

Les opérateurs devront non seulement installer les TMCT de Roskomnadzor au sein de leurs systèmes et fournir régulièrement des informations sur le routage à l'organisme de réglementation, mais ils devront aussi fournir à Roskomnadzor un accès à distance aux TMCT. Si l'organisme de réglementation considère qu'il existe une menace imminente contre la sécurité du réseau public de communication, il peut utiliser les TMCT pour imposer des modifications du routage du trafic, fermer et réserver des lignes et des canaux de communication, contacter directement les utilisateurs et modifier la configuration des communications. De fait, lorsque Roskomnadzor, de concert avec le ministère des Communications et le service fédéral de sécurité (FSB), déclare une urgence sur les communications, l'organisme de réglementation peut contrôler directement le routage et d'autres décisions des opérateurs.

Les exigences déclaratives comme les mesures d'urgence prévues par la loi de 2019 altéreront inévitablement l'interconnexion et le routage en Russie, et nuiront aux propriétés essentielles du Mode de fonctionnement du réseau Internet.

1 https://stat.ripe.net/RU

2 "On Amendments to the Federal Law 'On Communications' and the Federal Law 'On Information, Information Technologies and Information Protection'", 22 April 2019, http://publication.pravo.gov.ru/Document/Text/0001201905010025

3 Service fédéral de surveillance des communications, des technologies de l'information et des médias (Federal Service for Supervision of Communications, Information Technology, and Mass Media)

Quelles propriétés essentielles sont affectées par ces évolutions ?

Propriété essentielle n° 1 : une infrastructure ouverte et accessible dotée d'un protocole commun

Le modèle « sans autorisation » de plus petite barrière technique possible à l'entrée ne peut être réalisé qu'en l'absence de barrières techniques superflues pour se connecter à Internet. Cependant, la loi sur l'Internet souverain exige des opérateurs de réseau et des points d'échange Internet (IXP) qu'ils fournissent à l'organisme de réglementation des informations détaillées sur le routage ainsi que d'autres informations commerciales et opérationnelles. Cette exigence va bien au-delà des exigences normales pour l'obtention d'une licence commerciale, car elle implique de communiquer des informations techniques de manière continue. Elle semble exiger au quotidien un processus administratif très lourd pour la connexion à Internet et l'optimisation des modèles de connectivité. Les données requises sont souvent très dynamiques, en perpétuelle évolution en fonction des conditions locales, notamment en cas de modification du routage pour suivre le trajet le plus optimal, de défaillance d'un lien ou de redirection des flux de données via des liens de secours. Le décalage entre ce régime bureaucratique et la nature d'informations de ce type crée une barrière à l'ouverture et à l'accessibilité de l'infrastructure, et risque également d'entraver le processus décisionnel relatif à l'interconnexion, nuisant ainsi à la propriété essentielle n° 3.

Propriété essentielle n° 3 : gestion décentralisée et routage distribué

Cette propriété essentielle du Mode de fonctionnement du réseau Internet signifie que chaque réseau peut prendre des décisions indépendantes sur la manière de router le trafic vers ses voisins, en fonction de ses propres besoins, de son modèle commercial et des exigences locales. L'un des aspects les plus importants est l'absence de coordination ou de contrôle centralisé, chaque opérateur prenant ses propres décisions et collaborant librement avec les acteurs qu'il choisit.

L'obligation décrite ci-dessus pour les opérateurs d'informer l'organisme de réglementation des modifications du routage risque également d'entraver leur capacité opérationnelle à optimiser le routage au jour le jour, voire même en direct. Toute modification du routage susceptible d'être nécessaire pour des motifs opérationnels ou commerciaux implique désormais la communication d'informations potentiellement sensibles à l'organisme de réglementation. Il est impossible de savoir avec certitude si cette mesure s'appliquera aux modifications du routage en aval qui affectent le trajet de communication, ce qui est fréquent dans les opérations de réseau. Ainsi, un fournisseur d'accès à Internet (FAI) russe peut faire appel aux services d'un autre réseau pour permettre le transit de son trafic (c'est-à-dire en général la connexion à Internet dans son ensemble). Si ce fournisseur modifie son routage, un processus décisionnel algorithmique peut sélectionner un trajet faisant passer le trafic en dehors du pays, ce qui est perçu comme une menace susceptible de rendre ledit trafic vulnérable aux interceptions ou aux blocages. Les décisions opérationnelles de ce type sont constamment prises en temps réel, souvent par des partenaires contractuels, afin d'assurer la réactivité et la résilience du routage, mais cette nouvelle loi semble impliquer une procédure de notification déphasée par rapport au routage opérationnel du trafic.

La loi de 2019 nuit également à la gestion décentralisée des réseaux en permettant à l'organisme de réglementation de modifier à distance la configuration opérationnelle d'un réseau. Outre le fait de créer un point de défaillance unique et d'engendrer une incertitude opérationnelle, elle
risque d'avoir des conséquences imprévisibles, notamment des coupures et des failles de sécurité.

Durant un incident où l'organisme de réglementation estime être en présence d'une menace étrangère, les opérateurs risquent de ne pas être en mesure de contrôler leur propre routage. Certaines décisions d'interconnexion seront interdites et d'autres seront obligatoires, en fonction de décisions centralisées ne laissant pas aux opérateurs l'autonomie et la capacité nécessaires pour s'adapter aux conditions locales et aux besoins opérationnels et commerciaux.

De plus, les décisions centralisées sur le routage risquent, en situation d'urgence, d'être plus lentes et moins réactives ou agiles qu'à l'ordinaire, car l'organisme de réglementation devra effectuer des modélisations complexes

basées sur des données de sources multiples, pour certaines inadaptées ou obsolètes, afin de prendre des décisions pour un grand nombre d'opérateurs. Cela entraînera certainement une réaction plus lente, et peut-être même inadaptée, par rapport à une situation où chaque opérateur agit de façon indépendante en se basant sur sa propre interprétation en temps réel des conditions du réseau. Loin de gérer efficacement les menaces extérieures contre la sécurité, la stabilité et l'intégrité des systèmes de communication, cette mesure semble destinée à réduire la résilience, à allonger les délais de réaction et à réduire la qualité des réponses apportées.

Dans l'ensemble, la loi de 2019 nuit gravement à la gestion décentralisée du réseau et à la nature distribuée du routage du trafic Internet, à la fois en temps normal et en situation d'urgence. Cela entraînera une réduction considérable de l'agilité et la résilience du réseau, une mise à mal de l'autonomie et de l'expertise des opérateurs et une menace considérable contre la collaboration, l'optimisation de la connectivité et la portée mondiale nécessaires aux opérateurs comme aux utilisateurs d'Internet en Russie.

Interconnexion et routage en Chine

Trois opérateurs, China Telecom, China Unicom, et China Mobile, sont les fournisseurs d'accès à Internet dominants dans le pays et disposent de l'infrastructure nationale la plus complète. Ils desservent environ 70 % des utilisateurs d'Internet à haut débit en Chine et fournissent une grande partie du réseau dorsal utilisé par les plus petits fournisseurs d'accès. Ces trois entreprises contrôlent également la connectivité internationale et gèrent les passerelles de Pékin, Shanghai et Canton par lesquelles transite le trafic entrant et sortant de Chine. Hormis leur monopole sur les passerelles internationales, la domination d'un marché national par trois opérateurs n'est pas une situation unique à la Chine. Cependant, le régime d'interconnexion de ces entreprises, de même qu'entre elles et avec d'autres fournisseurs d'accès chinois, crée une topologie du réseau exceptionnellement hiérarchisée, qui nuit à la décentralisation de la gestion et à la distribution du routage.

Dans la plupart des pays, les grands opérateurs utilisent majoritairement des accords d'appairage de réseau sans acquittements (c'est-à-dire des accords ne donnant pas lieu à des transactions financières car les deux réseaux échangent des quantités de trafic similaires) plutôt que des interconnexions payantes pour gérer les flux de trafic entre eux. En Chine, cependant, les acquittements de frais d'interconnexion représentent la norme. Jusqu'au 1er juillet 2020, China Mobile, qui dispose d'un réseau Internet public légèrement moins important que les deux autres acteurs, a payé d'importants frais à China Unicom et China Telecom afin que son trafic puisse transiter sur leurs réseaux. Le ministère chinois des Technologies de l'information et de la communication vient de mettre un terme à l'acquittement de frais entre les trois grands opérateurs et leur a ordonné de réduire d'au moins 30 % les frais d'interconnexion qu'ils facturent à deux plus petits opérateurs de réseaux (China Broadcast Network et CITIC ASP). Cela rapproche les relations d'appairage entre réseaux en Chine des pratiques mondialement acceptées, mais souligne également le rôle central joué par l'État dans la planification du paysage de l'interconnexion et dans la définition de ses modèles tarifaires.

China Telecom, China Unicom, et China Mobile contrôlent à eux seuls la dorsale Internet nationale chinoise, et les autres fournisseurs d'accès doivent leur acheter le droit d'y accéder. De plus, les goulets d'étranglement détenus par ces trois entreprises sur l'interconnexion avec tous les réseaux hors de Chine limitent fortement l'accès des fournisseurs d'accès et des utilisateurs d'Internet à l'Internet mondial. En raison de la topologie (c'est-à-dire la structure) extrêmement hiérarchisée des réseaux chinois et du contrôle étroit et centralisé d'un nombre restreint de passerelles internationales, ce n'est pas avec l'Internet mondial que le pays entre en contact et interagit, mais seulement avec un sous-ensemble de celui-ci. L'inspection et le filtrage des données par les passerelles tendent également à ralentir le trafic international, limitant encore davantage les interactions avec l'Internet mondial. L'« Internet » chinois n'est pas connecté à Internet de façon significative, puisque ses réseaux centralisés et strictement contrôlés nuisent aux propriétés essentielles du Mode de fonctionnement du réseau Internet.

Quelles propriétés d'Internet sont affectées par ces dispositifs ?

Propriété essentielle n° 1 : une infrastructure ouverte et accessible dotée d'un protocole commun

La seule condition essentielle pour l'accès d'un nœud ou d'un réseau spécifique à Internet est l'utilisation des protocoles communs, notamment TCP/IP. Ce modèle « sans autorisation » de plus petite barrière technique possible à l'entrée est la base du développement rapide et de la portée mondiale d'Internet.

Le modèle chinois de routage et d'interconnexion, hiérarchisé et onéreux, ainsi que le système complexe de gestion des permis d'exploitation et de connexion à Internet des réseaux, impose des barrières si importantes qu'elles peuvent représenter un obstacle à l'accès. Malgré les récentes mesures visant à réduire les frais d'interconnexion élevés, la capacité des autres fournisseurs à créer leurs propres réseaux indépendants est très limitée du fait du contrôle de la dorsale nationale par les trois opérateurs majeurs. Le contrôle opérationnel centralisé de la dorsale nationale donne lieu à un système tellement fermé que les petits fournisseurs chinois n'ont pas vraiment de choix en matière d'interconnexion et d'optimisation de leurs flux de données.

De ce fait, l'infrastructure Internet chinoise n'est pas en mesure d'intégrer le plus vaste Internet mondial. Les goulets d'étranglement centralisés des trois opérateurs majeurs sur tous les points d'accès internationaux empêchent tout autre réseau d'accéder à l'Internet mondial de manière directe ou indépendante. Les réseaux ne peuvent pas réagir rapidement à l'évolution du trafic, des conditions économiques et de la demande des clients. Cela donne lieu à une structure de réseau non optimisée, à des tarifs élevés et à une faible résilience.

Sur Internet, le développement de l'infrastructure se fait de lui-même, tandis qu'en Chine, il est sujet à des règles et des conditions strictes imposées par le gouvernement afin d'en centraliser le contrôle. Cette incapacité des réseaux à offrir un accès mondial réduit l'intérêt global d'Internet pour ses utilisateurs qui n'ont pas accès à tout ce qu'offre l'Internet mondial. Les qualités du réseau défendues par la propriété essentielle n° 1, à savoir l'ouverture et la faiblesse des barrières d'entrée, sont fortement mises à mal, et les bénéfices en matière d'interopérabilité et de développement de l'infrastructure qu'elles pourraient engendrer ne sont donc pas pleinement accessibles aux utilisateurs d'Internet en Chine.

Propriété essentielle n° 3 : gestion décentralisée et routage distribué

Internet est un réseau de réseaux, sans coordination ni contrôle centralisé. La capacité des opérateurs à prendre des décisions indépendantes sur la façon de router le trafic permet à chacun d'eux de s'adapter rapidement aux nécessités opérationnelles et aux besoins des utilisateurs.

Le fonctionnement du routage en Chine est très éloigné de cet idéal. La structure hiérarchisée du réseau, qui permet aux opérateurs majeurs de gérer la dorsale nationale et de faire office de goulets d'étranglement pour l'accès international, réduit les possibilités d'interconnexion. Il semble n'exister aucun, ou très peu, d'appairage au trafic Internet en Chine, et l'interconnexion implique donc toujours l'acquittement de frais entre un nombre réduit d'acteurs dominants.

Le faible nombre d'acteurs dominants donne également lieu à une autre pratique inhabituelle : peu de réseaux disposent de leurs propres blocs d'adresses IP, et lorsque c'est le cas, la propriété du bloc d'IP est transférée au fournisseur en amont, qui définit et contrôle à sa place les routes de trafic utilisées par le petit réseau. Cela signifie que les petits réseaux ne disposent pas de la portabilité des numéros, c'est-à-dire qu'en passant d'un opérateur majeur à un autre, ils perdent leurs numéros IP ; ils sont donc pour ainsi dire bloqués.

Cette topologie hiérarchisée du réseau, par laquelle la plupart des décisions relatives au routage sont prises par les fournisseurs en amont, fait que les petits réseaux n'ont que peu ou aucun contrôle sur leurs politiques en matière de routage. Ils ne peuvent pas prendre de décisions opérationnelles en temps réel concernant l'ingénierie du trafic et ne peuvent qu'utiliser les routes par défaut que leur procurent les opérateurs majeurs. Cela réduit l'efficacité opérationnelle et la qualité de service pour les utilisateurs, car les décisions relatives au routage sont prises à un

niveau centralisé. Le manque d'agilité et d'autonomie, ainsi que le nombre déjà restreint de trajets de routage disponibles offerts par les opérateurs majeurs aux niveaux national et international, entraîne une moindre résilience.

Les opérateurs chinois doivent fonctionner avec une gestion centralisée et un routage concentré, ce qui est à l'opposé des propriétés permettant de rendre Internet agile, résilient et évolutif. Ils ne peuvent donc pas optimiser la connectivité, choisir librement les partenaires de réseau avec lesquels ils coopèrent, offrir une portée réellement mondiale aux utilisateurs, ni, semble-t-il, assurer une qualité de service optimale.

Le programme américain Clean Network

Le 5 août 2020, l'administration américaine a annoncé la création du programme « Clean Network », visant à atténuer les menaces contre « l'infrastructure technologique et de télécommunications essentielle des États-Unis » contre des « acteurs mal intentionnés, tels que le Parti communiste chinois (PCC) »[4].

Les cinq nouveaux axes de travail de Clean Network ciblent diverses facettes de l'écosystème Internet, de son infrastructure physique (câbles) et ses interconnexions de réseaux au stockage dans le cloud et aux applications.

Bien que la pleine portée du programme n'ait pas encore été dévoilée à l'heure où nous publions ce cas d'utilisation, les premières informations permettent de bien comprendre son impact sur plusieurs propriétés du Mode de fonctionnement du réseau Internet. Ce cas d'utilisation analysera l'exigence suivante du Clean Carrier : « veiller à ce que des opérateurs non fiables de la République Populaire de Chine (RPC) ne soient pas connectés aux réseaux de télécommunications des États-Unis. Les entreprises de ce type représentent une menace pour la sécurité nationale américaine et ne doivent pas offrir de services de télécommunications internationales vers et depuis les États-Unis. »

Quelles propriétés d'Internet sont affectées par ces dispositifs ?

Propriété essentielle n° 1 : une infrastructure ouverte et accessible dotée d'un protocole commun

Les mesures visant à atténuer les menaces pour la sécurité et la confidentialité des données en transit peuvent entraîner une restriction de l'interconnexion avec les opérateurs chinois, interdisant de fait l'interconnexion directe avec la Chine, car seuls ces opérateurs assurent la connectivité internationale de l'Internet chinois. Comme l'a déclaré Ted Hardie dans sa réaction aux mesures proposées, « l'interconnexion de différents réseaux est la base physique sur laquelle reposent Internet et tous les services et possibilités qu'il offre. En entravant cette interconnexion, cette initiative porte un coup au cœur d'Internet en tant qu'entreprise. Elle le met également en danger d'autres manières, qui auront un certain nombre de conséquences inattendues et néfastes »[5].

Comme dans les autres cas où les interconnexions sont dictées par une politique centralisée au lieu d'être basées sur les besoins d'un opérateur de réseaux et de ses clients, cette situation risque fort d'amoindrir l'efficacité de l'infrastructure. Du fait de la restriction de l'interconnexion directe entre les réseaux chinois et américains, le trafic entre les nœuds chinois et américains devra emprunter des trajets non optimaux ou effectuer un détour, ce qui aura un impact négatif sur les performances et la résilience d'Internet.

Propriété essentielle n° 3 : gestion décentralisée et routage distribué

Sur le plan du routage d'Internet, la restriction envisagée n'atteint pas l'objectif annoncé. Si le trajet des données passe d'un nœud situé aux États-Unis à la Chine, sa gestion par un opérateur de RPC est inévitable, à moins que le but soit de couper totalement ce type de trajet. De ce fait, il sera nécessaire de prendre une route moins optimale

4 Annonce de l'expansion du « Clean Network » pour protéger les intérêts américains, https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets/

5 Réflexions sur le Clean Network program, https://medium.com/@ted.ietf/thoughts-on-the-clean-network-program-5f1c43764152

impliquant d'autres réseaux. Cela entraînera une latence plus importante et une moindre résilience, sans répondre à la menace perçue aux extrémités.

Si l'objectif est d'éviter les opérateurs de RPC susceptibles de transmettre du trafic qui n'est pas destiné à la Chine et n'en provient pas, comme cela a été le cas lors d'un incident de routage en 2010[6], les mesures envisagées n'atténuent pas cette menace. Du fait de la nature du système de routage d'Internet, les incidents de ce type ne nécessitent pas une interconnexion directe entre un opérateur de RPC et un réseau américain. Ainsi, une fuite de route provoquée par un réseau suisse en 2019 a accidentellement envoyé du trafic à d'autres réseaux en passant par China Telecom[7]. Bien qu'elle soit absurde, la solution ultime à ce problème serait d'interdire la connexion à des opérateurs de RPC à tous les autres réseaux d'Internet. Cependant, il est peu probable que d'autres pays acceptent cette solution, car cela limiterait également leur propre capacité à se connecter à la Chine. Le fait de tenter d'empêcher d'autres pays d'accéder à Internet est tout simplement une autre forme d'attaque contre ses propriétés essentielles. La vraie solution aux problèmes auxquels cherche à répondre Clean Network ne consiste pas à contrôler les interconnexions, mais à veiller à ce que BGP, le protocole de routage d'Internet, fonctionne de manière sécurisée. L'une des façons d'y parvenir est de mettre en œuvre les mesures recommandées par MANRS afin de soutenir la sécurité et la résilience du routage[8].

Même si le programme Clean Network ne traite pas du routage, il amène à se demander comment les réseaux américains devraient gérer les annonces de routage issues d'opérateurs de RPC. La seule réponse logique est de gérer les annonces de ce type conformément à la norme du BGP et aux pratiques de sécurité du routage mondialement acceptées, par exemple en vérifiant l'exactitude de l'annonce de routage par l'utilisation de RPKI (Resource Public Key Infrastructure, un système qui permet l'authentification des annonces de route). Toute politique de routage artificielle imposée aux opérateurs de réseau aura un effet négatif sur la résilience, la stabilité et la portée mondiale d'Internet dans son ensemble.

Conclusion

L'évolution de l'interconnexion et du routage que décrivent les tendances de ce cas d'utilisation est bien éloignée de l'idéal exprimé par le Mode de fonctionnement du réseau Internet. De ce fait, beaucoup des bénéfices potentiels, surtout en matière de collaboration, de portée mondiale et de résilience, ne sont pas optimisés.

Le modèle du réseau chinois ne permet pas l'application de propriétés essentielles qui génèrent une part importante de la valeur d'Internet. Même si la taille du marché intérieur chinois donne aux utilisateurs d'Internet les moyens de se passer de la valeur de l'Internet mondial, d'autres pays qui adopteraient ce modèle passeraient à côté des innombrables possibilités de collaboration, de connectivité et de développement économique qu'il apporte.

Les mesures russes visant à centraliser le contrôle du routage et à formaliser un « interrupteur » pour la connexion à l'Internet mondial enfreignent deux des propriétés essentielles du Mode de fonctionnement du réseau Internet et réduisent la résilience de ce dernier en cas de crise. Si cette approche venait à se répandre, la capacité d'Internet à offrir un vaste ensemble d'avantages en termes de collaboration, de portée mondiale et de développement économique à d'autres pays pourrait s'en trouver sérieusement menacée.

Les mesures du programme Clean Network annoncées par l'administration américaine auront un effet négatif sur l'infrastructure d'interconnexion et les flux de trafic, ce qui engendrera une baisse des performances et de la résilience et pourrait entraîner un affaiblissement de la sécurité pour les utilisateurs du monde entier.

---

6 La Chine détourne-t-elle 15 % du trafic Internet ? Plutôt environ 0,015 %, https://www.forbes.com/sites/andygreenberg/2010/11/19/china-hijacks-15-of-internet-traffic-more-like-015/

7 Tu ne devineras jamais où les données mobiles européennes ont été reroutées pendant deux heures. Oh. En fait, si. Oui, vers China Telecom, https://www.theregister.com/2019/06/10/bgp_route_hijack_china_telecom/

8 Normes mutuellement agréées pour la sécurisation du routage, https://www.manrs.org/