Comment isoler son Internet ?

Par **Kavé SALAMATIAN**
Professeur d'informatique à l'Université de Savoie-Mont Blanc

L'Internet forme aujourd'hui un élément incontournable du monde contemporain. C'est le principal vecteur de la révolution numérique qui est en train de changer profondément nos sociétés. Ce réseau est le support d'un nombre croissant de services et d' « organismes d'importance vitale » (OIV). Mais l'Internet est aussi le support de ce cyberespace dans lequel une part croissante de notre vie sociale et économique est projetée. Ainsi, Internet et les réseaux qui le constituent font aujourd'hui partie des équipements stratégiques des États.

Les États souhaiteraient étendre la portée de leur souveraineté à ce réseau. Mais cela n'est pas une tâche aisée. Nous avons pu constater ces dernières années de nombreuses déconnexions globales d'Internet d'un pays qui ont été motivées par des raisons visiblement légères, comme la protection contre la fraude aux examens de l'enseignement secondaire. La raison évoquée pour la plupart des déconnexions ont été la sécurité nationale ou la protection de la population dans le contexte de révolte locale ou nationale. Une étude intéressante [(1)] questionne l'efficacité de ces mesures et montre que loin de réduire les tensions, les coupures à large échelle les attisent. Ces éléments montrent que les coupures Internet infligent au pays un coût économique, social et politique qu'il est difficile de contrebalancer avec un quelconque bénéfice direct. Cela montre la possibilité d'isoler l'Internet d'un pays, mais cet isolement brutal aboutit fréquemment à l'inverse de l'effet escompté.

Les dernières années ont aussi vu la résurgence de la question du maintien de la souveraineté des États sur l'Internet. Mais la souveraineté suppose la capacité d'action sur le réseau à l'échelle d'un pays. Cet article suivra une démarche cyberstratégique afin d'étudier la portée du contrôle des États sur la composante d'Internet qui se trouve sur leur territoire. Cette étude permettra de caractériser plusieurs catégories d'approches suivies par différents États sur la souveraineté de l'Internet.

On peut définir la cyberstratégie en paraphrasant la définition classique de la stratégie : « l'art de positionner, diriger et gouverner ses cyberforces dans le cyberespace afin d'atteindre ses cyberobjectifs ». Il convient donc de déterminer l'espace des « cyber-objectifs », de répertorier les « cyber-forces » en présence, et de délimiter le champ de manœuvre dans le « cyberespace » relatif à la question de l'isolation de l'Internet.

Les cyberobjectifs

L'Internet est une composante stratégique pour les États. La révolution numérique a mis « en ligne » une large palette de services qui étaient traditionnellement gérés « hors ligne ». La connectivité Internet est donc devenue nécessaire, voire vitale pour un nombre croissant de services de l'économie et de l'État. Mais la mondialisation signifie que la connectivité n'a pas seulement une portée nationale et que les échanges internationaux ont donc une importance considérable, que ce soit pour les OIV ou les autres acteurs économiques. Mais l'importance de la connectivité internationale est contrebalancée par des régulations et des enjeux géopolitiques. Un premier « cyber-objectif » est de garantir pour les services d'importance vitale, ainsi que pour

(1) https://theconversation.com/shutting-down-social-media-does-not-reduce-violence-but-rather-fuels-it-115960

la totalité de l'économie une connectivité intérieure et, quand cela est souhaitable, internationale, dans la limite des régulations et enjeux géopolitiques.

Un second élément à considérer est que l'Internet répond aussi à des besoins de communication qui, sans être vitaux, ont néanmoins une importance sociale et politique considérable. La liberté d'expression et la fluidité d'échange de l'information ont une incidence sur la confiance des citoyens vis-à-vis de leur gouvernement, et de leur environnement économique. Mais la connectivité est à double tranchant, puisqu'elle permet aussi à des acteurs malicieux, externes ou internes, d'interférer avec la confiance des citoyens vis-à-vis de leur gouvernement. L'équilibre entre les bénéfices sociaux, politiques et économiques de la libre circulation des informations, avec les risques de cette ouverture en termes de perte confiance ou de contrôle de l'information qui circule sur les réseaux, est un second « cyber-objectif ».

Un dernier élément est lié à la cybersécurité. Ces dernières années ont été le cadre d'attaques d'États contre des infrastructures considérées comme vitales dans d'autres États. Le virus Stuxnet ciblant le programme nucléaire iranien, les cyberattaques attribuées à la Russie contre l'Estonie en 2007, la Géorgie en 2009 et en 2020, ainsi que l'Ukraine en 2017 et 2018, en sont des exemples. Les États s'inquiètent aussi d'attaques qui pourraient être lancées par des cybercriminels, des acteurs mafieux ou même des groupes terroristes. Ces craintes sont un autre élément dans la définition de leurs cyberobjectifs.

Les choix d'équilibres entre des impératifs contradictoires au cœur des cyberobjectifs sont éminemment politiques. Se poser la question d'isoler l'Internet d'un pays, ou d'appliquer un quelconque niveau de souveraineté sur celui-ci, a un très fort poids politique et est un indicateur de la cyberstratégie de l'acteur.

Cyberforces en présence

La définition des cyberobjectifs permet de dégager certaines des cyberforces : les OIV, les régulateurs, les organes de sécurité, les acteurs économiques, et aussi les citoyens. Il faut ajouter à ceux-ci les opérateurs de réseaux, les fournisseurs de services informatiques, les entreprises du numérique, mais aussi les universités, les organismes de formation et la recherche industrielle et académique.

Les opérateurs de réseaux fournissent, *in fine,* la connexion à Internet qui va être le support sur lequel les autres acteurs, ou cyberforces, vont s'appuyer. Historiquement, les États ont suivi le monopole d'un acteur étatique de télécommunications à l'intérieur d'un pays ou d'une région. Ce modèle, qui est encore suivi dans de nombreux pays, souffre de prix élevés par manque de compétition, et d'incapacité d'investissement, alors que l'activité de fournisseurs de services réseau est très gourmande en capitaux. Les opérateurs doivent déployer de coûteuses infrastructures qu'il faut amortir rapidement pour suivre l'évolution rapide des technologies.

Ce modèle tend à être remplacé au profit d'un modèle concurrentiel avec plusieurs acteurs actifs sur un territoire. Mais ce marché compétitif reste sous le contrôle d'autorités de régulation, dont les prérogatives sont variables : strictement économiques parfois, ou plus globales dans certains pays. Mais l'intégration de fournisseurs de services étrangers est un sujet sensible. Les acteurs étrangers sont nécessaires, car ils amènent des capitaux essentiels. Ils fournissent aussi la connectivité internationale. Cependant, ils posent aussi des problèmes de juridictions applicables, de sécurité, ou encore de prise de position stratégique. Pour ces raisons, certains pays interdisent la présence d'acteurs étrangers, en les obligeant parfois à apparaître sous le couvert de « chaperons » locaux.

Alors que certains États considèrent l'élément économique des réseaux indépendamment des implications sécuritaires, d'autres mettent ces dernières au centre de la décision. Certains

considèrent l'Internet comme un tout, « un espace informationnel », englobant aussi bien les aspects d'infrastructures techniques que les services s'y déployant et les informations y circulant, ainsi la totalité de cet espace doit être gérée par une autorité centrale qui a la prérogative de toutes les décisions s'y appliquant [2]. D'autres États organisent l'Internet en compartiments : l'infrastructure, les contenus, les questions de sécurité informatique et/ou de sécurité de l'État [3], qui sont régulés indépendamment.

Les réseaux résultent généralement d'un phénomène d'émergence, c'est-à-dire un processus non dirigé d'interactions microscopiques entre acteurs plus on moins indépendants qui crée un résultat macroscopique concret. La structure du réseau est le résultat de l'interaction individuelle et microscopique d'acteurs qui décident d'investir pour s'interconnecter, mais aussi du cadre global de régulation qui limite l'espace des actions possibles. Quand aucune régulation n'est appliquée, les acteurs ont tendance à construire des réseaux qui possèdent des propriétés dites de « petit monde », c'est-à-dire une faible distance moyenne entre les nœuds ainsi que des cliques de nœuds fortement interconnectés entre eux [4]. Le dilemme du prisonnier, où les acteurs ne peuvent facilement évaluer les coûts et les bénéfices d'une coopération (mise en place d'un lien fiable et à haut débit) ou d'une défection (déconnexion du lien ou réduction de la qualité de service offerte par surutilisation des ressources), qui est à la base de la décision d'interconnecter deux nœuds, peut expliquer ces structures. Ainsi, les acteurs minimisent leurs coûts de connexion tout en se protégeant de la défection des partenaires en multipliant les connexions. Ces structures sont résilientes par construction. Par contre, l'existence de régulations particulières peut pousser les acteurs vers des structures qui sont beaucoup plus fragiles. Par exemple, l'obligation des opérateurs de passer par un seul point de connexion à l'international rend le contrôle du trafic très simple, mais rend ce réseau extrêmement vulnérable à une attaque de déni de service ciblant ce point de passage. Les décisions de régulation relatives aux réseaux sont complexes et des effets « papillon », où l'application d'une décision locale « anodine » génère des effets imprévus à grande échelle, apparaissent fréquemment, par exemple l'effet Streisand, où la suppression d'un contenu jugé offensant aboutit à une très large distribution de celui-ci alors qu'il n'aurait eu qu'une portée très limitée sans la censure. La décision d'isoler un réseau peut sembler évidente sur l'instant au vu d'impératifs à courte vue, mais elle peut s'avérer plus coûteuse que le risque qui avait motivé la décision.

Les fournisseurs de services informatiques, c'est-à-dire les fournisseurs d'informatique en nuage (*cloud providers*) et les points d'échange réseau (*Internet eXchange Providers*), sont d'autres acteurs importants. Ils sont fréquemment rattachés aux fournisseurs de services réseau, mais sont parfois des acteurs indépendants ou des associations d'usagers. Ils jouent un rôle fondamental dans la résilience des réseaux en fournissant des chemins alternatifs au cas où des pannes ou des attaques bloqueraient les chemins principaux. Mais l'existence de ces acteurs nécessite une certaine libéralisation du marché, en particulier vis-à-vis des étrangers qui peuvent amener des capitaux financiers, ce qui peut aller à l'encontre de l'impératif de contrôle. Cette tension existe en Afrique, où un grand nombre d'IXP communautaires ont été construits ces dernières années permettant une densification de l'Internet. Mais ils sont tributaires pour la plupart de l'aide du gouvernement chinois qui a offert « gratuitement » des équipements Huawei.

(2) La Chine est un exemple d'un tel État, ou la CAC (Cyberspace Authority of China) est en charge de toutes les dimensions du cyberespace, sous la direction directe du président chinois.
(3) La France développe cette approche avec l'Autorité nationale de régulation des télécommunications en charge de la régulation des opérateurs technique, l'ANSSI en charge de la sécurité informatique, et la direction générale de la Sécurité intérieure en charge des aspects relatifs à la sécurité de l'État, en particulier du terrorisme et de l'espionnage.
(4) FALOUTSOS Michalis, FALOUTSOS Petros & FALOUTSOS Christos (1999), "On power-law relationships of the Internet topology", *SIGCOMM Comput. Commun. Rev.* 29, 4, october, pp. 251–262, doi: https://doi.org/10.1145/316194.316229

L'isolation de l'Internet n'a de sens que s'il existe en interne suffisamment de services et de contenus. Or, cela nécessite l'émergence d'une économie numérique dans le pays, qui dépend elle-même de l'existence de la connectivité et d'une circulation fluide de l'information. Ainsi, la volonté de contrôle de l'Internet peut être un obstacle à l'émergence d'un écosystème économique actif autour du réseau.

Le champ de manœuvre du cyberespace

Revenons à la question initiale : peut-on isoler l'Internet d'un pays ? Ou, plus précisément, peut-on réduire l'espace d'action des cyberforces en présence sans infliger des dégâts insoutenables ? Un acteur malicieux se poserait la question duale : peut-on infliger des dégâts maximaux en réduisant le champ d'action des acteurs par des cyberattaques ?

Même s'il existe plusieurs moyens d'agir sur la connectivité, il est néanmoins possible d'établir une taxonomie globale des structures de contrôle.

Dans les pays qui ont gardé un cadre de régulation inspiré du monopole d'un opérateur d'État, la connectivité internationale est généralement centralisée en un ou plusieurs points bien identifiés. Dans ces pays, la déconnexion et l'isolement du réseau sont relativement simples, car il suffit de déconnecter ces points de connexion. Mais le manque de diversité à l'intérieur de ces pays signifie qu'une coupure des liaisons internationales équivaut à l'arrêt de toutes les activités de l'économie numérique. De plus, la concentration de la connectivité en un nombre limité de points fragilise le réseau, car un acteur malveillant peut faire tomber le réseau de la totalité d'un pays en s'attaquant à ces points.

Dans les pays possédant un écosystème numérique plus riche, la coupure de l'Internet est plus complexe et nécessite des mécanismes particuliers appelés communément « *kill switch* ». Ces mécanismes regroupent en un point central le contrôle de la totalité des réseaux de communication. Cette approche n'est pas simple à mettre en œuvre, car elle suppose la coopération de tous les acteurs, nationaux ou internationaux de l'écosystème numérique. Plusieurs États, la Chine et l'Iran par exemple, ont des clauses légales et même constitutionnelles s'assurant que la dorsale du réseau appartient au gouvernement et est donc totalement sous son contrôle. Néanmoins, ces régulations présupposent que l'État ait les capacités d'investissement et l'agilité nécessaires afin de soutenir la croissance de la demande de trafic sur la dorsale.

Serait-il possible d'assurer un contrôle fort de la connectivité Internet d'un pays, tout en permettant l'existence d'un riche écosystème d'acteurs qui serait le terreau d'une économie numérique locale et florissante ? C'est cette quadrature du cercle que visent beaucoup d'États totalitaires, mais aussi un certain nombre de pays occidentaux.

La Chine est dans la catégorie des pays qui ont mis en place un cadre de régulation stricte limitant l'activité des acteurs étrangers. L'État chinois a depuis l'arrivée d'Internet en 1987 séparé son Internet en trois parties : le réseau interne, le réseau extérieur et les passerelles, ou espaces tampons. Le réseau Internet est sous le contrôle total de l'État, en particulier la dorsale du réseau doit appartenir à l'État. Le contenu est filtré à l'entrée par ce que l'on nomme « le grand pare-feu de Chine », et la surveillance y est omniprésente. Les acteurs étrangers ne peuvent s'installer directement à l'intérieur du réseau chinois, mais ont le droit de s'installer dans un nombre limité de zones tampons qui sont situées à Hong Kong, mais aussi en plusieurs points intérieurs, qui même s'ils sont géographiquement à l'intérieur de la Chine, sont *de facto* à l'extérieur, car situés au-delà du grand pare-feu. Cette structuration a été conçue dès le début par l'État chinois. On ne peut donc considérer l'architecture du réseau chinois comme résultant d'un phénomène d'émergence d'acteurs indépendants, comme cela a été le cas dans la plupart des autres pays, mais comme le résultat d'une conception. L'interconnexion de l'Internet

chinois avec le monde extérieur se fait complètement par le biais d'acteurs gouvernementaux qui contrôlent le grand nombre de points d'interconnexion de la Chine avec le monde extérieur, en particulier la dizaine de points d'arrivée des câbles maritimes et terrestres internationaux.

En parallèle, le gouvernement chinois a promu le développement d'une économie numérique nationale par le biais de politiques protectionnistes s'appuyant sur l'action du grand pare-feu, comme l'interdiction d'accès à Facebook ou à Twitter, et un ralentissement majeur des outils de Google, la mise en place des mécanismes incitatifs de développement d'acteurs du numérique comme Lenovo, premier constructeur d'ordinateurs au monde, ou Huawei, deuxième constructeur de routeurs et premier constructeur de *smartphones*, tous deux entreprises d'État qui ont été cédées à des acteurs privés, une stratégie ambitieuse de formation d'ingénieurs informaticiens, et un investissement très important dans la recherche académique et privée. La Chine pourrait aujourd'hui se déconnecter de l'Internet mondial, si elle le souhaitait, car elle a dès le début mis en place une architecture visant à dissocier son réseau interne du monde extérieur, a développé une économie nationale numérique florissante, et a planifié et défini sa cyberstratégie de façon centralisée par le biais de la CAC (China Authority of Cyberspace*)*, qui est sous l'autorité directe du président chinois. Mais la Chine préfère pour des raisons économiques et stratégiques rester en intégration avec l'Internet mondial.

Quid des pays qui n'ont pas mis en place dès le début des contraintes architecturales et réglementaires ? Dans ce cas, il faut transformer une architecture existante qui est généralement le résultat d'un processus. Cette reconstruction est très coûteuse, car elle nécessite un changement sur un réseau en cours d'opération. Néanmoins, plusieurs pays souhaitent s'engager dans ce processus. On peut citer la Russie qui, depuis la loi promulguée fin 2019, vise à développer un « Ru.net », qui pourrait être déconnecté de l'Internet mondial. Néanmoins, la volonté politique n'est pas suffisante, et la tâche est immense. Le réseau Internet russe a eu une croissance importante durant les années 1990 et a suivi une croissance assez anarchique. Kevin Limonier décrit l'histoire de cette émergence dans un livre [(5)]. Cela a abouti à une architecture de réseau très riche qu'il est très difficile de contrôler, ce que l'étendue territoriale du pays ne simplifie pas. L'État russe a dû, fin 2019, faire un test grandeur nature de déconnexion afin de pouvoir répertorier les services informatiques qui dépendent de la connectivité internationale. Ainsi, même si la Russie a clairement la volonté de restructurer son réseau, elle a encore un long chemin avant d'y arriver.

Néanmoins, un pays, l'Iran, a réussi à restructurer son réseau afin d'aboutir simultanément à un contrôle total et à grain fin de son réseau, et à un riche écosystème de connectivité permettant un niveau de résilience élevé. Comme dans beaucoup d'autres pays, l'Internet est arrivé en Iran par le biais des universités et des organismes de recherche [(6)]. L'Internet iranien a connu une croissance rapide, mais il est aussi apparu de façon croissante comme un risque pour les fondements du régime. À partir de la Révolution verte de 2009, le gouvernement iranien s'est lancé dans un vaste projet de censure des contenus. Mais c'est le virus Stuxnet, attribué aux États-Unis, qui a fourni l'argument principal pour restructurer totalement son réseau afin de le rendre résilient aux attaques, tout en le rendant plus facilement contrôlable. Cette restructuration, qui a pris environ dix ans, est aujourd'hui opérationnelle. Elle a été mise en œuvre sous l'égide de « l'autorité centralisée de l'espace virtuel », qui a regroupé en un point de décision toutes les décisions relatives à l'architecture. Nous avons décrit dans le détail ce processus dans un article [(7)].

(5) LIMONIER Kevin (2018), *Ru.net : géopolitique du cyberespace russophone*, collection « Les carnets de l'Observatoire », n°4, juin.
(6) L'Institut de physique et de mathématiques (IPM) de Téhéran a été le précurseur de l'Internet en 1994 et reste encore aujourd'hui le porteur du DNS « .ir ».
(7) SALAMATIAN Loqman, DOUZET Frederick, LIMONIER Kevin & SALAMATIAN Kavé, "The geopolitics behind the routes data travels: a case study of Iran", https://arxiv.org/abs/1911.07723

Mais le cas iranien reste une exception. Ce cas n'aurait pas été possible sans les sanctions internationales, puis américaines, qui ont rendu impossible la présence d'acteurs internationaux en Iran, à l'exception notable de Rostelecom qui par le biais du câble EPEG (Europe-Persia Express Gateway) [8] profite de la position géostratégique de l'Iran. Les sanctions ont en grande partie rendu plus difficile l'émergence d'une économie numérique avec des connexions à l'international, et ont obligé les cybernautes iraniens à se rabattre sur des solutions informatiques locales en dépit de leur grande méfiance vis-à-vis de celles-ci. Ainsi, la restructuration de l'Internet a été possible par l'action conjointe et en ciseaux de la volonté du gouvernement iranien de contrôler le réseau, et des sanctions, en particulier américaines, qui rendent toute alternative impossible.

Conclusion

Cet article nous a permis de faire le point sur la question de la souveraineté et du contrôle de l'Internet. Nous avons emprunté une approche de cyberstratégie afin de répondre à la question « Peut-on isoler son Internet ? ». Cette approche montre qu'il est possible pour les États de prendre le contrôle de leur réseau. Néanmoins, cela a un coût important, car il faut combiner une forte volonté politique, l'adaptation de l'environnement de régulation ainsi que de l'environnement de l'économie du numérique. Ainsi, le coût de cette prise de contrôle peut facilement dépasser le bénéfice escompté, et même être contreproductif. Il faut donc réfléchir à ces questions avec une vision stratégique, globale et à long terme, car le fait de se positionner sur certaines de ces questions peut avoir des impacts dépassant largement le cadre initial.

(8) https://www.vodafone.com/business/carrier-services/connectivity/submarine-terrestrial-cable/EPEG