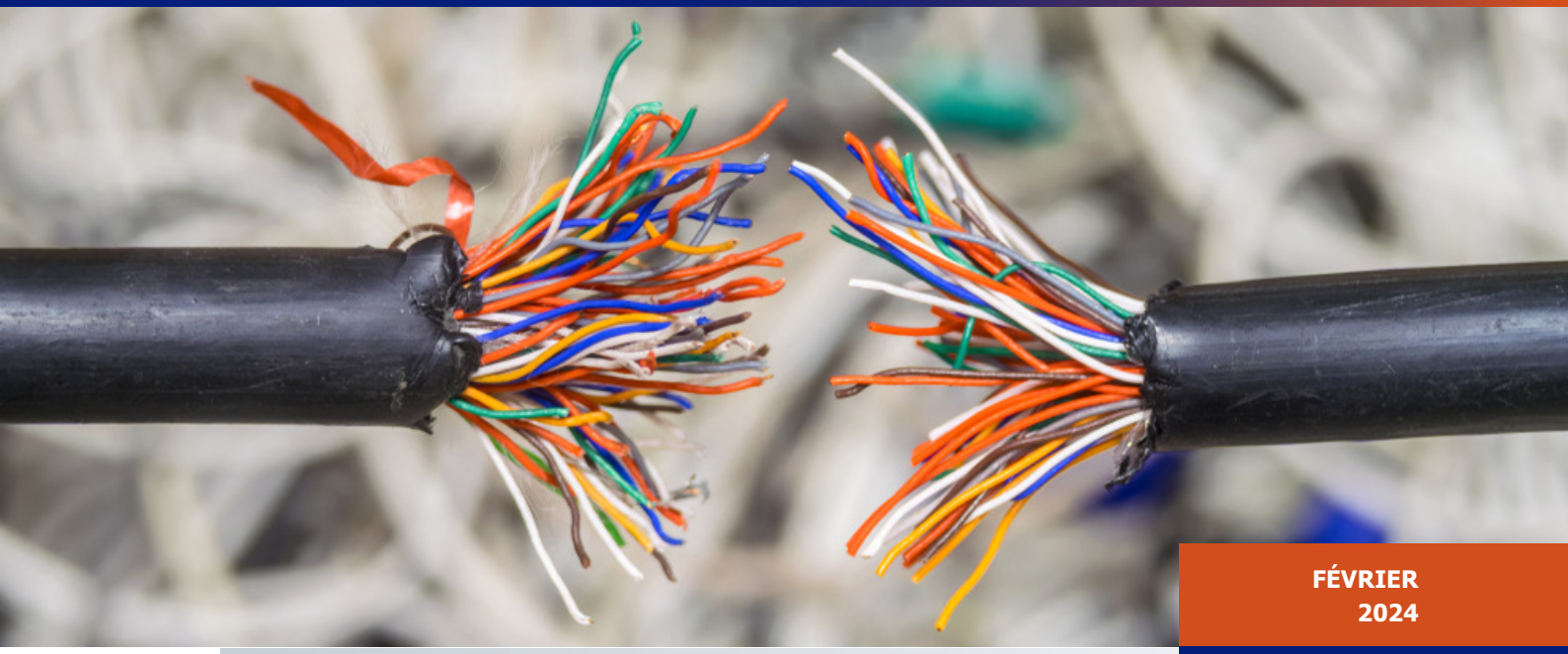
ÉTUDES
DE L'IFRI

CENTRE GÉOPOLITIQUE DES TECHNOLOGIES



FÉVRIER
2024

Un Internet en morceaux ?

Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne

Julien NOCETTI

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une fondation reconnue d'utilité publique par décret du 16 novembre 2022. Elle n'est soumise à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

ISBN : 979-10-373-0836-8

Comment citer cette publication :
Julien Nocetti, « Un Internet en morceaux ? Fragmentation d'Internet et stratégies de la Chine, la Russie, l'Inde et l'Union européenne », *Études de l'Ifri*, Ifri, février 2024.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Site internet : Ifri.org

Auteur

Julien Nocetti est chercheur associé à l'Institut français des relations internationales (Ifri) et membre du centre GEODE (Géopolitique de la Datasphère – Université Paris 8). Docteur en sciences politiques, il a été chercheur à l'Ifri entre 2009 et 2019, et enseignant-chercheur à l'Académie militaire de Saint-Cyr Coëtquidan entre 2019 et 2023. Il est membre du comité de rédaction de la revue *Études françaises de renseignement et de cyber* et membre du conseil d'orientation stratégique du CIGREF. Ses travaux portent, d'une part, sur les problématiques numériques internationales (diplomatie du numérique et de l'intelligence artificielle, cyber-conflictualité) ; d'autre part, sur la politique étrangère de la Russie, en particulier sur ses stratégies numériques et cyber.

Résumé

De la pandémie de Covid-19 aux ramifications de l'invasion russe de l'Ukraine, l'actualité technologique réveille le spectre d'une fragmentation accélérée de l'Internet global. La « fragmentation » d'Internet est l'idée d'un émiettement du réseau des réseaux, voire de la sécession de certaines parties d'Internet. Elle décrit la segmentation du réseau global et sa tendance à sa régionalisation. Cette étude examine la manière dont les principales puissances, à travers leurs politiques nationales et étrangères, sont susceptibles d'accélérer, volontairement ou non, cette fragmentation. Le rôle des acteurs privés, notamment les grandes plateformes du numérique, doit également être considéré.

L'étude analyse, d'abord, les différents types de fragmentation : technique, (géo)politique et commerciale. La fragmentation technique résulte de décisions qui, délibérément ou non, de façon permanente ou temporaire, rompent ou limitent la connectivité numérique entre une partie d'Internet et le reste du réseau. Les propositions de protocoles et standards alternatifs à ceux déjà utilisés à l'échelle mondiale rentrent dans cette catégorie. La fragmentation (géo)politique découle quant à elle de pratiques diverses : localisation des données, coupures volontaires d'Internet, politique visant à exclure les entreprises chinoises de l'ensemble des couches d'Internet, et notamment des infrastructures de connectivité, etc. En parallèle, depuis les années 2010, se développe l'idée d'une fragmentation économique et commerciale, mue par des stratégies protectionnistes de la part des autorités nationales, le développement de logiques propriétaires et l'exploitation des données d'utilisateurs captifs par les grandes plateformes du numérique. En bâtissant leur propre infrastructure, les plateformes créent en quelque sorte leur propre réseau, tout en devenant la porte d'entrée principale vers l'Internet global.

L'étude souligne que si Internet a longtemps été présenté par la diplomatie américaine comme une infrastructure globale afin de défendre ses propres intérêts, l'instrumentalisation de son ossature, privatisée, représente désormais l'un des déterminants-clés des dynamiques de « fragmentation ». Elle examine ensuite les politiques menées par la Chine, la Russie, l'Inde et l'Union européenne, dont les initiatives, mues par des ambitions très diverses, sont également porteuses de reconfigurations d'Internet. Celles-ci sont en effet multiples et reflètent les visions distinctes du capitalisme numérique portées par ces acteurs étatiques.

Executive summary

From the Covid-19 pandemic to the ramifications of Russia's invasion of Ukraine, international events are fueling fears of an accelerated fragmentation of the global Internet. Internet "fragmentation" refers to the idea of a crumbling of the network of networks or even the secession of certain parts of the Internet. It describes the segmentation of the global network and its tendency towards regionalization. This study examines how major powers, through their national and foreign policies, are likely to accelerate this fragmentation, whether voluntarily or not. The role of private players, notably the major digital platforms, is also considered.

The study begins by analyzing the different types of fragmentation: technical, (geo)political and commercial. Technical fragmentation results from decisions that, deliberately or not, permanently or temporarily, break or limit digital connectivity between one part of the Internet and the rest of the network. Proposals for alternative protocols and standards to those already in use worldwide fall into this category. (Geo)political fragmentation stems from various practices: data localization, voluntary Internet cuts, policies aimed at excluding Chinese companies from all layers of the Internet, particularly from connectivity infrastructures, and so on. At the same time, since the 2010s, the idea of economic and commercial fragmentation has emerged, driven by protectionist strategies on the part of national authorities, the spread of proprietary software and hardware, and the exploitation of captive user data by major digital platforms. By building their own infrastructure, platforms create their own network while becoming the global Internet's main gateway.

The study underlines that while U.S. diplomacy has long supported the global nature of the Internet infrastructure as part of its national interests, the instrumentalization of its privatized backbone now represents one of the critical determinants of the dynamics of "fragmentation". The study then examines the policies pursued by China, Russia, India and the European Union, whose initiatives, driven by diverse goals, are also reconfiguring the Internet. Indeed, these initiatives are manifold, reflecting the distinct visions of digital capitalism these state actors hold.

Sommaire

INTRODUCTION 6

SÉMANTIQUE ET ENJEUX D'UNE RÉCURRENTE FRAGMENTATION D'INTERNET 8

La possibilité d'une partition 8

Trois nuances de fragmentation 10

Fragmentation technique 11

Fragmentation (géo)politique 14

Fragmentation commerciale 17

La fragmentation, une problématique qui concerne principalement les États-Unis ? 17

UNE AUTRE LECTURE DE LA FRAGMENTATION D'INTERNET : LES INITIATIVES DE QUATRE ACTEURS 20

Chine : une stratégie globale de fragmentation 20

Imposer les standards techniques du futur 20

Hardware *: des exportations tous azimuts au croisement de la géopolitique et du commerce 22*

Applications : WeChat et la logique de couches de fragmentation 23

Russie : en marche vers une scission de l'Internet mondial 24

La quête d'une indépendance numérique 25

Guerre en Ukraine et fragmentation 26

Inde : une fragmentation partielle ? 27

Industrie numérique, données : à la recherche d'une souveraineté 27

Des relations complexes avec la tech américaine et chinoise 28

Une ambivalence dans les négociations internationales 29

Union européenne : la quête d'une « souveraineté numérique » sans fragmentation d'Internet 30

Le droit plus fort que la « fragmentation » ? 30

Vers une autonomie stratégique par les infrastructures ? Le projet DNS4EU 31

CONCLUSION 33

Introduction

Dans un rapport de juillet 2022, le groupe de travail du Council on Foreign Relations (CFR) chargé de réfléchir à l'avenir de la diplomatie américaine du numérique livrait une réflexion sans équivoque des écueils de la politique de Washington dans ce domaine. « L'ère de l'Internet global est révolue » ouvre le propos, suivi du constat qu'Internet serait désormais « plus fragmenté, moins libre et plus dangereux » qu'une décennie auparavant[1]. Reflet d'un vague à l'âme conjoncturel ou traduction de profonds questionnements, cette évolution invite à examiner la manière dont les principales puissances affectent l'écosystème mondial d'Internet, à travers leurs politiques nationales et étrangères.

Récurrente dans les débats relatifs à Internet depuis près de deux décennies et plus récemment au champ numérique et technologique, la « fragmentation » découle du phénomène de compartimentation d'Internet qui marque sa territorialisation progressive par les États. Cette évolution contredirait la nature historique d'Internet – espace ouvert, neutre et continu qui, dans la vision de ses fondateurs, plaçait en son cœur les caractéristiques de décentralisation, d'anonymat, de disponibilité et d'égalité entre les utilisateurs[2].

Distinguons d'emblée Internet (l'infrastructure, soit le réseau des réseaux) du Web (sa couche applicative, lieu du *consumer Internet*), au sein desquels les logiques de fragmentation divergent. Resserré voire verrouillé dans un certain nombre de pays (Chine, Russie, Iran, Corée du Nord, Cambodge, Myanmar, etc.), le contrôle étatique du réseau Internet tend à fragiliser sa continuité et augmente fortement les risques pour les populations concernées : répression politique, atteintes aux droits de l'homme et à la vie privée. Là où certains plaident, face à la domination historique des États-Unis, en faveur d'un rééquilibrage du réseau mondial, les États autoritaires souhaitent plutôt obtenir la maîtrise physique d'un espace qui risquerait de leur échapper et d'où pourraient venir des menaces, internes et/ou externes.

À cette fragmentation du réseau répond un éclatement du Web, au sein duquel l'utilisateur évolue entre des espaces plus ou moins hétérogènes. Pour remédier aux enfermements algorithmiques (favorisant la diffusion de

1. N. Fick et J. Miscik (dir.), « Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet », Council on Foreign Relations, *Independent Task Force Report*, n° 80, juillet 2022, p. 7, disponible sur : www.cfr.org.

2. Lire par exemple F. Turner, *Aux sources de l'utopie numérique. De la contre-culture à la cyberculture, Stewart Brand un homme d'influence*, Caen, C&F Éditions, 2012 ; et B. Loveluck, *Réseaux, libertés et contrôle. Une généalogie politique d'internet*, Paris, Armand Colin, coll. Le temps des idées, 2015.

fausses nouvelles et les bulles informationnelles) qui isolent les internautes les uns des autres, la portabilité des données, la transparence et l'interopérabilité des services sont les prérequis à un Web ouvert assurant une connectivité globale.

Déjà donc présente, la fragmentation concerne des espaces différents et son interprétation diverge selon les acteurs. Quoi qu'il en soit, l'analyse de la fragmentation d'Internet est indissociable de la description de logiques régaliennes traversant le champ du numérique – logiques portant au pinacle une « souveraineté numérique » ardemment souhaitée par les différents acteurs du jeu international[3].

De la pandémie de Covid-19 aux ramifications de l'invasion russe de l'Ukraine, l'actualité technologique internationale est riche d'illustrations d'une fragmentation en marche. Le contentieux transatlantique au sujet du transfert des données, la politique chinoise de mise à l'agenda de ses propres standards Internet, les spéculations sur l'interdiction du réseau social chinois TikTok aux États-Unis, mais aussi les stratégies d'investissement des grands acteurs du numérique américains et chinois, réveillent, à des degrés divers, le spectre d'une fragmentation accélérée d'Internet.

Plutôt que de considérer la fragmentation d'Internet comme le prélude à un « découplage » total des réseaux, cette étude envisage celle-ci comme un long processus de « re-connectivité » qui modèle la configuration d'Internet de sorte à peser sur les flux de données échangés entre les différents acteurs. La compétition sino-américaine innerve – et domine – ce paradigme qui agrège une quadruple dimension géopolitique, technologique, juridique et commerciale. Dans ce cadre, le discours sur la fragmentation est ambigu. Il décrit une multitude de phénomènes complexes et complémentaires, autant qu'il sert à maintenir un *statu quo* favorable aux intérêts de politique étrangère et économique américains dans les enceintes internationales de gouvernance de l'Internet. La présente étude dépasse néanmoins la focale des États-Unis en comparant les initiatives d'acteurs nationaux – Chine, Russie, Inde et Union européenne. Les politiques de ces acteurs peuvent s'apparenter à des logiques de fragmentation, bien que la nature différente des régimes politiques ne permette de dresser des tables d'équivalence.

3. Voir J. Nocetti (dir.), « Souveraineté numérique : dix ans de débats, et après ? », *Annales des Mines – Enjeux numériques*, n° 23, septembre 2023.

Sémantique et enjeux d'une récurrente fragmentation d'Internet

La possibilité d'une partition

Le terme de « fragmentation » d'Internet est régulièrement discouru au moyen du vocabulaire de la partition. L'idée d'un émiettement du réseau des réseaux, voire de la sécession de certaines parties d'Internet, renvoie le plus souvent au terme de « balkanisation ». Le terme, utilisé depuis les années 1940 dans les débats constitutionnels et commerciaux aux États-Unis, fait référence au processus de morcellement d'un État en plus petites entités indépendantes, et revêt sans surprise une acception négative. Associé à Internet, il apparaît pour la première fois en 1997 dans une étude du Massachusetts Institute of Technology (MIT). Marshall van Alstyne et Erik Brynjolfsson développent alors l'idée que la croissance d'une infrastructure globale de communication ne conduirait pas nécessairement à l'émergence d'un « village mondial de l'Internet » – elle pourrait aussi fragmenter les sociétés et « balkaniser » les interactions dans l'espace numérique naissant[4].

Le terme de balkanisation trouve un nouvel élan dans le contexte du premier Sommet mondial sur la société de l'information (SMSI) en 2005 à Tunis, sous l'égide des Nations unies. Le sommet est l'aboutissement de près de quatre ans de négociations portant sur la participation des différents acteurs (États, sociétés civiles, acteurs privés) à l'élaboration des règles s'appliquant à Internet. Il voit poindre l'opposition qui deviendra structurante entre les positions portées par les régimes autoritaires et celles défendues par les partisans d'un modèle multi-acteurs garant des valeurs d'ouverture et d'interopérabilité véhiculées par les fondateurs d'Internet. Les voix d'intellectuels comme le juriste américain Tim Wu – qui souligne la façon dont la censure et les contraintes réglementaires peuvent conduire à balkaniser Internet[5] –, ou l'entrepreneur japonais Joichi Ito, qui alerte sur les hypothétiques conséquences de l'internationalisation de la gestion du

4. M. van Alstyne et E. Brynjolfsson, « Electronic Communities: Global Village or Cyberbalkans? », Massachusetts Institute of Technology, mars 1997, disponible sur: https://web.mit.edu.

5. J. Goldsmith et T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, New York, Oxford University Press, 2006. Voir aussi T. Wu, « The Filtered Future », Slate, 11 juillet 2005, disponible sur : https://slate.com. Tim Wu suggère ainsi que les internautes ne visitent pas régulièrement les sites web d'autres pays, que les sites comme Google deviennent nationaux (à l'étranger) à l'aide de logiciels de géolocalisation, et que le trafic local augmente particulièrement rapidement en Chine (continentale) par rapport au trafic échangé *via* ses routes internationales.

système de noms de domaine (DNS) pour l'unité d'Internet[6], relaient de premières inquiétudes.

La description d'un « Splinternet » vient se superposer à la « balkanisation ». Contraction de *split* (diviser) et Internet, celui-ci désigne une partie d'Internet qui ferait sécession et deviendrait dès lors inaccessible aux autres composantes du réseau, pour des raisons technologiques, commerciales ou politiques. Employé dès 2001 par l'expert libertarien Clyde Wayne Crews, il décrit alors plus un idéal – créer des Internets parallèles gérés de façon privée et autonome pour révéler les potentialités infinies de l'Internet[7] – qu'un phénomène défiant les fondamentaux techniques et politiques du réseau mondial. La défense de l'individu-consommateur fonde cette vision qui trouve un écho parmi les communautés originelles d'Internet : plutôt que d'évoluer dans un cyberespace liberticide, qui s'atrophie à mesure que les États tentent de le réglementer (lutte contre le spam, limitation de l'accès à certains types des contenus, etc.), les consommateurs devraient s'organiser dans des réseaux propriétaires détenus par des entreprises leur permettant d'accéder à du contenu et des services personnalisés[8].

Le terme trouve une nouvelle dynamique en 2010. John Bernoff, président de l'institut d'études Forrester Research, considère que la prolifération de terminaux, de systèmes d'exploitation et d'applications qui ne sont pas interopérables signe l'échec de l'utopie de l'Internet collaboratif et ouvert[9]. Censé favoriser l'« aplatissement » du monde, Internet devient à l'inverse la matrice d'un nouveau paradigme dans lequel les logiques propriétaires de certains acteurs en voie de position dominante voire oligopolistique – Apple, Google, Amazon, etc. – compliquent la sortie des utilisateurs. Cet argumentaire rejoint la description d'une remise en cause par les fournisseurs d'accès du principe de la neutralité du Net, lequel préconise une égalité de traitement des données qui circulent – peu importe leur contenu, la plateforme utilisée ou le destinataire – sans aucune restriction imposée par les acteurs de l'économie numérique[10]. La notion d'« *enclosure* » sert précisément à décrire les stratégies d'exploitation des données d'utilisateurs captifs par les grandes plateformes du numérique[11].

6. J. Ito, « The Internets », Blog de Joichi Ito, 11 juillet 2005, disponible sur : https://joi.ito.com.
7. C. W. Crews, « One Internet Is Not Enough », CATO Institute, 11 avril 2001, disponible sur : www.cato.org.
8. *Ibid*. Voir aussi M. Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge (MA), MIT Press, 2010.
9. J. Bernoff et S. van Boskirk, « The Splinternet », Forrester, 26 janvier 2010, disponible sur : www.forrester.com.
10. *Ibid*.
11. B. Pajot, « Des barbelés sur la prairie Internet : contre les nouvelles enclosures, les communs numériques comme leviers de souveraineté », Ministère des Affaires étrangères, août 2020, disponible sur : www.diplomatie.gouv.fr.

Plus largement, la description d'une segmentation du réseau global illustre la ligne de crête sur laquelle celui-ci évolue en permanence, entre difficile maintien de son universalité et tendance à sa régionalisation[12]. Pour certains, cette dichotomie rejoue le vieux débat entre l'utopie d'une démocratisation de la société et d'une libération de l'information *via* Internet, et la collision de la « révolution de l'information » avec les règles instituées par les États[13].

Enfin, liée à la fragmentation, la notion d'« alignement » désigne selon Milton Mueller les processus délibérés ou non conduisant à une centralisation croissante d'Internet à l'échelle nationale, par le biais de différents ressorts : la sécuritisation de celui-ci selon des ambitions gouvernementales, la territorialisation des flux de données et les initiatives visant à structurer le contrôle des ressources critiques d'Internet dans un cadre étatique[14]. Les partisans de cette démarche s'opposeraient alors à l'autorégulation d'Internet, processus qualifié de multi-parties prenantes qui repose sur un critère participatif aux mécanismes de gouvernance de l'infrastructure et des usages d'Internet[15]. Cet « alignement » d'Internet avec les juridictions étatiques a trouvé une illustration quasi paroxystique au moment des révélations d'Edward Snowden sur l'étendue de l'espionnage numérique des États-Unis, celui-ci suscitant alors un vaste mouvement de réactions politiques dans le monde[16]. En outre, depuis les attentats de 2015-2016 ayant visé la France et ses voisins européens, l'ajustement des lois nationales aux dispositifs de contrôle d'Internet rejoue cette problématique d'alignement. L'emploi croissant des technologies de surveillance numérique se généralise au sein des démocraties (déploiement de systèmes de contrôle automatisés aux frontières, de prévision policière et de systèmes de reconnaissance faciale), traduisant un renforcement du recours à des instruments éprouvés.

Trois nuances de fragmentation

La fragmentation d'Internet peut revêtir différentes formes, et l'évaluation de la menace qu'elle représente pour le réseau global varier en fonction de la manière de conceptualiser Internet – d'une stricte infrastructure technique à une sphère publique globalisée. La profusion de réflexions décrivant une fragmentation d'Internet n'a cependant pas conduit à un consensus sur la nature du processus de division à l'œuvre ni sur le degré d'urgence à y remédier.

12. S. Malcomson, *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web*, New York, OR Books, 2016.
13. F. Tréguer, *L'Utopie déchue : une contre-histoire d'Internet, XVe-XXIe siècle*, Paris, Fayard, 2019.
14. M. Mueller, *Will the Internet Fragment?*, Cambridge, Polity, 2017.
15. B. de La Chapelle, « Gouvernance Internet : tensions actuelles et futurs possibles », *Politique étrangère*, vol. 77, n° 2, Ifri, été 2012, p. 252-253, disponible sur : www.cairn.info.
16. J. Nocetti, « Puissances émergentes et internet : vers une troisième voie ? », *Politique étrangère*, vol. 79, n° 4, Ifri, hiver 2014, p. 43-55.

Fragmentation technique

La fragmentation technique demeure l'angle par lequel les risques d'éclatement du réseau global sont le plus souvent analysés. L'approche de certains se veut extensive. Ce type de fragmentation est ainsi défini par Milton Mueller comme :

> « la défaillance *intentionnelle* [de l'Internet mondial], menée par un groupe d'acteurs capables d'entraîner avec eux *un segment significatif de la population mondiale* ; cette défaillance doit parvenir à établir des *incompatibilités techniques* effectives entre "leur" partie de l'Internet et le reste [du réseau]. Ces incompatibilités doivent être à la fois *durables* et capables d'*entraver les communications entre les parties qui sont désireuses de communiquer*. »[17]

Pour d'autres, le volet technique de la fragmentation de l'Internet doit se focaliser sur les risques qui pèsent sur l'interopérabilité du réseau et sur les entraves techniques au transfert des données[18]. En substance, donc, elle résulte de décisions qui, délibérément ou non, de façon permanente ou temporaire, rompent ou limitent la connectivité numérique entre une partie de l'Internet et le reste du réseau.

Samuele Dominioni regroupe les processus de fragmentation technique autour des risques de sécurité pouvant affecter les principales ressources d'Internet que sont :

- le nommage (gestion de l'espace de noms de domaine – *Domain Name System*, le DNS, socle technique de l'édifice Internet),
- l'adressage (attribution de numéros de protocoles de communication et de numéros de réseaux IP physiques)
- et le routage des données[19].

Les enjeux liés à l'adressage ont été identifiés dès la décennie 2000 : dans *Protocol Politics*, Laura DeNardis montrait comment la raréfaction progressive des adresses IPv4 avait suscité des stratégies étatiques d'investissement dans l'IPv6, technologie plus récente et alors non dominée par les intérêts et les entreprises américains[20]. Or, l'adoption encore sporadique du protocole IPv6[21] renforce le processus de fragmentation en

17. M. Mueller, *Will the Internet Fragment?*, *op. cit.*, p. 43. Italiques dans l'original.
18. W. Drake, V. Cerf et W. Kleinwächter, « Internet Fragmentation: An Overview », World Economic Forum, janvier 2016, p. 4, disponible sur : www.weforum.org.
19. S. Dominioni, « Internet Fragmentation and Cybersecurity: A Primer », UNIDIR, 2023, disponible sur : https://unidir.org.
20. L. DeNardis, *Protocol Politics: The Globalization of Internet Governance*, Cambridge (MA), MIT Press, 2009, p. 97-138.
21. Cartographiée et mise à jour par les équipes de Google, l'adoption de l'IPv6 traduit de réelles disparités : en janvier 2024, seuls cinq pays dépassent les 60 % d'adoption (France, Allemagne, Inde, Malaisie, Arabie saoudite). Voir www.google.com.

raison de l'incompatibilité technique entre l'IPv4 et celui-ci[22]. Le manque de réactivité des fournisseurs d'accès dans la transition vers l'IPv6 est critiqué en particulier aux États-Unis, où ceux-ci ont cherché à éviter les coûts relatifs à une mise à niveau en matière d'interopérabilité[23]. Enfin, le processus de configuration de terminaux *via* l'IPv6 est susceptible d'accroître les vulnérabilités numériques et, plus largement, la surface d'attaque[24].

Autre enjeu identifié concernant l'adressage : l'hypothèse que des *Internet Protocols* nationaux sans coordination ou en conflit direct avec le système existant viennent perturber significativement l'accessibilité et la sécurité des réseaux nationaux. Dans une telle optique, les États seraient contraints de nouer des accords bilatéraux avec les fournisseurs d'accès et d'assurer la sécurité des protocoles et standards de leurs propres réseaux[25].

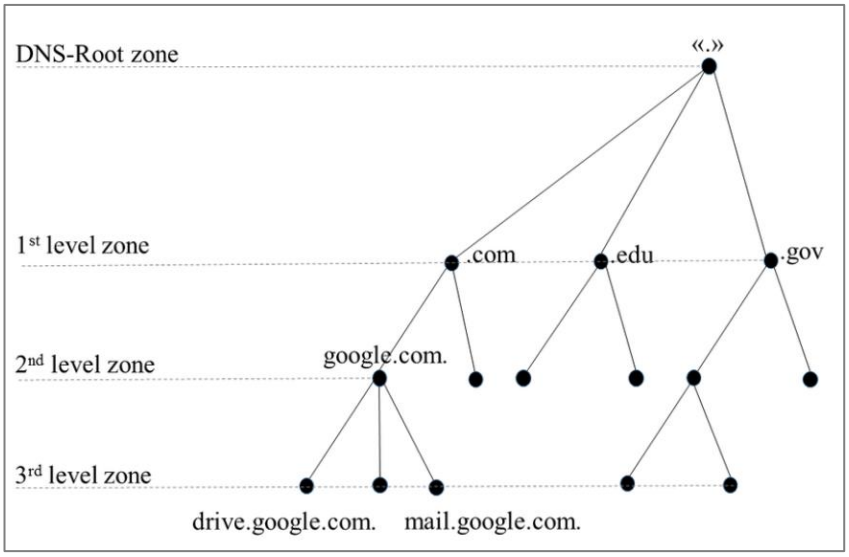
La question du nommage a pour l'essentiel souligné les menaces qui pèsent sur le système de noms de domaine (DNS), un système hiérarchique permettant de constituer des adresses IP sous forme de mots intelligibles au lieu d'une suite de chiffres. La zone racine du DNS (*DNS root zone*) correspond à la zone DNS dite de plus haut niveau dans le système de noms de domaine de l'Internet. Elle renvoie aux serveurs de noms pour les domaines de premier niveau (*Top-Level Domain*, ou TLD : les .com, .org, mais aussi les codes-pays comme le .fr, le .jp, etc. Cf. schéma page suivante). Les noms de domaine ont la propriété d'être traduits en une ou plusieurs adresses IP, et ces adresses peuvent être modifiées sans changer le nom de domaine. Ainsi, si un site Web choisit de localiser un serveur à une nouvelle adresse IP, il n'est pas nécessaire de changer de nom de domaine. La zone racine du DNS est contrôlée par treize « identités » ou grappes de serveurs racines du DNS qui font autorité pour les requêtes aux domaines de premier niveau. Douze organismes contrôlent ces serveurs : neuf américains, deux européens et un japonais. En outre, pour neuf de ces serveurs, l'architecture technique est répartie dans des lieux géographiques divers : en janvier 2024, il y a ainsi 1 756 sites dans 59 pays qui hébergent un serveur racine du DNS[26].

Le fait qu'une société de droit californien (l'Internet Corporation for Assigned Names and Numbers – ICANN) ait assuré, entre 1998 et 2016 *via* un lien contractuel avec le Département du Commerce américain, la gestion de la racine du DNS, de l'attribution des adresses IP et la maintenance des protocoles du système avec l'Internet Engineering Task Force (IETF), a placé un enjeu de supervision technique au cœur de multiples débats dans les

22. E. Bais, « IPv4 vs IPv6: What Security Professionals Should Know », Prefix Broker (non daté), disponible sur : www.prefixbroker.com.
23. J. Force Hill, « Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers », John F. Kennedy School of Government, Harvard University, printemps 2012, p. 22-24, disponible sur : www.belfercenter.org.
24. Voir par exemple « Transition vers IPv6 », communiqué de l'ARCEP et de l'Internet Society France, 18 décembre 2019, disponible sur : www.arcep.fr.
25. S. Dominioni, « Internet Fragmentation and Cybersecurity: A Primer », *op. cit.*, p. 11.
26. Données compilées sur le site https://root-servers.org.

enceintes internationales chargées de débattre des contours d'une « gouvernance » mondiale de l'Internet[27].

Architecture logique du DNS



Source: R. G. Alakberov et al.*, "Internationalized Top Level Domain Names: Their Registration and Problems",* Problems of Information Society*, 2017, n° 1, p. 45.*

Vaste et complexe, l'enjeu du DNS a cristallisé de nombreuses craintes liées à sa fragmentation, tant par le développement de « segments nationaux » que par les revendications portées par certains États en faveur d'une dé-américanisation des mécanismes de gestion des ressources critiques d'Internet[28]. À titre d'exemple, en 2010, une coalition menée par la Russie, avec la Chine, avait soumis à l'Union internationale des télécommunications (UIT) une proposition visant à accorder aux États un pouvoir de véto sur les décisions adoptées par le conseil d'administration de l'ICANN sur les problématiques de nommage et d'adressage. Moscou et Pékin ont coordonné leurs efforts pour obtenir la même année la création de noms de domaine de premier niveau nationaux en caractères non latins, dans un effort concomitant pour promouvoir un Internet multilingue[29]. Soulignons par ailleurs que les tentatives de lancer une concurrence à l'ICANN sur la racine d'Internet ne bénéficient que d'un suivi modeste : ainsi le protocole RINA (*Recursive InterNetwork Architecture*), conçu en 2008

27. Voir J. Nocetti (dir.), « Internet, une gouvernance inachevée », *Politique étrangère*, vol. 79, n° 4, Ifri, hiver 2014, p. 10-81.
28. Voir F. Musiani, D. Cogburn, L. DeNardis et N. Levinson (dir.), *The Turn to Infrastructure in Internet Governance*, New York, Palgrave Mcmillan, 2016.
29. A. Bhuiyan, *Internet Governance and the Global South. Demand For a New Framework*, Basingstoke, Palgrave Mcmillan, 2014, p. 97-112.

par John Day comme alternative au TCP/IP des origines, n'a été adopté en partie que par l'Arménie et le Vatican[30].

Enfin, la topologie d'Internet est garantie par le *Border Gateway Protocol* (BGP), qui assure la fonction de routage du réseau global, c'est-à-dire permettre de relier entre eux la multiplicité des sous-réseaux qui composent l'Internet, donc d'assurer l'acheminement des données produites d'un point A à un point B. Ces vastes routes d'Internet suscitent elles aussi des convoitises étatiques et peuvent mener à une dynamique de fragmentation. Pour la Russie et l'Iran, par exemple, la maîtrise des chemins qu'empruntent les données leur confère plusieurs avantages que leurs autorités viseront à exploiter : filtrer, espionner ou détourner le trafic des données[31]. En raison de sa sophistication et de son manque de transparence, l'architecture BGP est aisément manipulable à des fins stratégiques. Elle l'est également sur un plan concurrentiel, avec des implications porteuses de fragmentation : « la concentration du trafic des données autour de quelques acteurs majeurs du routage et de grandes plateformes comme Google, Facebook ou Amazon » questionne la liberté de circulation des données, leur intégrité et leur souveraineté, à plus forte raison lorsque les pannes de certains de leurs services se multiplient[32]. Enfin, la démocratisation des réseaux virtuels privés (VPN) est parfois assimilée à une forme de fragmentation, dans la mesure où les utilisateurs de ceux-ci s'isolent de l'Internet global ; à l'inverse, certains États limitent ou interdisent l'usage de protocoles VPN pour empêcher leurs citoyens d'anonymiser leur trafic Internet[33].

Fragmentation (géo)politique

Le caractère (géo)politique de la fragmentation se nourrit de la territorialisation croissante d'Internet. Produit d'une confusion rhétorique, la fragmentation d'Internet décrirait pour Milton Mueller le mouvement d'« alignement » d'Internet par les États sur leurs frontières nationales. Lutte de pouvoir au sujet de l'avenir de la notion même de souveraineté dans un monde numérisé, le débat sur la fragmentation dépasse le seul champ d'Internet et de sa supervision technique pour embrasser des logiques fondamentalement géopolitiques[34].

30. J.-A. Fines, « RINA, un projet pour l'internet de nouvelle génération », *La Revue européenne des médias et du numérique*, 24 septembre 2019, disponible sur : https://la-rem.eu.
31. Sur le cas russe, voir K. Limonier, « Vers un 'Runet souverain' ? Perspectives et limites de la stratégie russe de contrôle de l'Internet », *Echo*Géo (en ligne), n° 56, 2021, disponible sur : https://journals.openedition.org. Sur la stratégie iranienne, voir L. Salamatian, F. Douzet, K. Salamatian et K. Limonier, « The Geopolitics Behind the Routes Data Travel: A Case Study of Iran », *Journal of Cybersecurity* (en ligne), vol. 7, n° 1, 2021, disponible sur : https://academic.oup.com.
32. F. Douzet, « La panne de Facebook révèle l'urgence de penser des solutions pour favoriser la décentralisation d'Internet », *Le Monde*, 11 octobre 2021, disponible sur : www.lemonde.fr.
33. W. Drake, V. Cerf, W. Kleinwächter, « Internet Fragmentation: An Overview », *op. cit.*, p. 24.
34. M. Mueller, *Will the Internet Fragment?*, *op. cit.*, p. 3.

En ce sens, la maîtrise des données est devenue la question sur laquelle cette fragmentation politique se révèle la plus tangible. Le dogme de la libre circulation des données (*free flow of data*) – socle de la convergence entre la mondialisation économique et l'essor du numérique – a été et reste contesté à plusieurs échelles et selon des modalités variables, par des régimes autoritaires et des États démocratiques. Tournant majeur, les révélations de Snowden en juin 2013 ont illustré cette remise en cause croissante de l'affranchissement des cadres nationaux. La politisation des pratiques de localisation des données personnelles est dès lors devenue un enjeu de souveraineté nationale et de compétition internationale[35].

Pour les États, le droit sert à légitimer cette territorialisation d'Internet. Les réponses différenciées de ceux-ci correspondent dans une large mesure à la nature des régimes politiques concernés. Quand certains États – principalement autoritaires – privilégient une localisation physique des données personnelles sur leur territoire –, d'autres États comme le Brésil ont préféré contraindre par la loi les entreprises qui collectent, stockent ou traitent des données personnelles des citoyens du pays à respecter la loi brésilienne sur le respect de la vie privée[36].

Outre le recours à des instruments juridiques, les politiques étatiques pour conserver la maîtrise des données produites par leurs ressortissants ont également consisté à soutenir le développement d'acteurs nationaux, tout particulièrement dans le *cloud*, à limiter les investissements étrangers dans l'industrie des *data centers*, voire à dupliquer les données des ressortissants sur le territoire national[37]. Les détracteurs de ces types de mesures les dénoncent comme participant à la fragmentation d'Internet, que ces mesures soient de nature protectionniste (ajuster les règles d'une compétition asymétrique avec les grands acteurs technologiques américains), sécuritaire (se défendre d'une surveillance étrangère) ou géopolitique (dénoncer les actions offensives des États-Unis dans le cyberespace[38]).

Si les pratiques de localisation des données ne sont pas nécessairement pensées pour « fragmenter » Internet, les coupures volontaires d'accès au réseau global (*Internet shutdowns*) supposent un acte délibéré. Phénomène en hausse, les coupures volontaires d'Internet concernaient 35 pays en 2022 (187 actes cette année-là contre 159 en 2020). Selon l'organisation non

35. T. Gomart, J. Nocetti et C. Tonon, « L'Europe, sujet ou objet de la géopolitique des données ? », *Études de l'Ifri*, juillet 2018, disponible sur : www.ifri.org.

36. M. Maciel et B. Martins dos Santos, « Brésil : un *soft power* numérique », in A. Pannier (dir.), « Les politiques technologiques des puissances numériques moyennes », *Études de l'Ifri*, février 2023, p. 24-25, disponible sur : www.ifri.org. Voir aussi A. Cattaruzza, « Quelle souveraineté pour l'espace numérique ? », *in* S. Taillat, A. Cattaruzza et D. Danet (dir.), *La Cyberdéfense. Politique de l'espace numérique*, Paris, Armand Colin, 2018, p. 88-89.

37. T. Gomart, J. Nocetti, C. Tonon, « L'Europe, sujet ou objet de la géopolitique des données ? », *op. cit.*, p. 19.

38. W. Drake, V. Cerf, W. Kleinwächter, « Internet Fragmentation: An Overview », *op. cit.*, p. 41-45 ; J. Force Hill, « Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers », *op. cit.*, p. 46-47.

gouvernmentale (ONG) Access Now, entre janvier et mai 2023, 21 États ont pris l'initiative de coupures (au nombre de 80) : s'il s'agit principalement de régimes autoritaires (Chine, Russie, Iran, etc.), l'Inde est le pays qui suspend le plus l'accès à Internet, pour des raisons variées (éviter des réponses violentes dans des provinces faisant l'objet de luttes séparatistes comme au Cachemire, mais aussi empêcher la triche lors des examens[39]). Des régions subissant des conflits voire des guerres civiles, comme le Myanmar ou le Tigré en Éthiopie, sont aussi et régulièrement déconnectées de l'Internet global par leurs autorités[40]. Si ces pratiques restent essentiellement documentées lors d'épisodes de tensions et de crises politiques aiguës, comme en Iran en 2019 puis à partir de septembre 2022[41], les coupures volontaires revêtent des implications concrètes pour les populations concernées en matière d'accès à l'emploi, à des revenus ou même à de la nourriture. En Inde par exemple, l'accès à l'Internet mobile conditionne souvent l'accès aux applications qui ouvrent des droits en matière de protection sociale, de droit du travail et d'obtention de rations alimentaires[42]. Au demeurant, si le *kill switch* s'apparente à un geste souverain ultime, il révèle surtout une incapacité des décideurs qui y recourent à étendre la souveraineté étatique à la sphère numérique[43].

Le processus de « territorialisation » d'Internet se joue enfin dans le domaine stratégique. La constitution de capacités offensives pour produire des effets sur la scène internationale est palpable lors de conflits militaires, que ce soit pour prendre le contrôle des infrastructures physiques d'un réseau (comme en Ukraine[44]), ou pour détruire l'infrastructure Internet d'un pays ainsi que les moyens de connectivité mobile (comme à Gaza à partir d'octobre 2023[45]). Cette dimension de la fragmentation, encore peu étudiée, présente cependant des risques bien réels pour la stabilité et la résilience du cyberespace.

39. Voir « An Overview of Global Internet Shutdowns », Access Now, 19 mai 2023, disponible sur : www.accessnow.org ; « Who Is Shutting Down the Internet in 2023? A Mid Year Update », Access Now, 31 juillet 2023, disponible sur: www.accessnow.org.
40. « Internet Shutdowns Have Become a Weapon of Repressive Regimes », *The Economist*, 15 octobre 2021, disponible sur : www.economist.com.
41. M. Burgess, « Iran's Internet Shutdown Hides a Deadly Crackdown », Wired, 23 septembre 2022, disponible sur : www.wired.com.
42. « "No Internet Means No Work, No Pay, No Food" Internet Shutdowns Deny Access to Basic Rights in "Digital India" », rapport des ONG Human Rights Watch et Internet Freedom Foundation, 2023, disponible sur : www.hrw.org.
43. M. Mueller, *Will the Internet Fragment?, op. cit.*, p. 91.
44. Pour une lecture des manipulations par la Russie du protocole BGP en Ukraine depuis 2014, voir F. Douzet *et al.*, « Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) during the Ukrainian Crisis », in *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade*, Tallinn, NATO CCDCOE, 2020, p. 157-182.
45. M. Burgess, « The Destruction of Gaza's Internet Is Complete », Wired, 27 octobre 2023, disponible sur : www.wired.com.

Fragmentation commerciale

Au-delà des justifications géopolitiques de la fragmentation, les enjeux d'ordre économique ne peuvent être sous-estimés, qu'il s'agisse de stratégies protectionnistes de la part des autorités nationales (par exemple en Chine ou aux États-Unis) ou bien de stratégies strictement commerciales. Lié au modèle économique des grandes plateformes du numérique – des recettes publicitaires corrélées à des fichiers de données d'internautes –, cette dynamique commerciale incite des acteurs comme Meta ou Google à renforcer leur socle technologique propriétaire afin de retenir leurs usagers et monétiser les contenus produits et échangés.

Ces écosystèmes technologiques se sont constitués en « jardins clôturés » (*walled gardens*) opaques et instituant des relations de complète dépendance chez les utilisateurs. La maîtrise de ces données constitue une source de revenu stratégique qui pousse ces entreprises à restreindre leurs échanges de données, voire à rendre incompatible toute recherche ou tout échange de données réciproques. Ainsi, Google et Meta (Facebook, Instagram, WhatsApp) bloquent mutuellement tout transfert de données entre leurs différentes applications depuis 2010.

Cette fragmentation commerciale renvoie enfin au processus de « plateformisation » d'Internet, qui concerne les acteurs les plus consolidés de l'économie numérique, incités à bâtir et posséder leur propre infrastructure technique. Ainsi, en déployant leurs propres câbles sous-marins, en installant leurs protocoles conçus en interne sur des technologies propriétaires, accompagnés d'un accès direct aux données de milliards de consommateurs captifs, Google, Meta ou Amazon créent en quelque sorte leur propre réseau, tout en devenant la porte d'entrée principale vers l'Internet global[46]. Catalyseurs d'une fragmentation concernant les données et les infrastructures, les entreprises du Web et les acteurs des télécommunications sont par ailleurs concernés par l'enjeu de la neutralité du réseau et du respect de la propriété intellectuelle[47].

La fragmentation, une problématique qui concerne principalement les États-Unis ?

La triple nature de la fragmentation d'Internet, par-delà les logiques souveraines qui traversent avec insistance le réseau global, n'est pas décorrélée de l'évolution de la politique étrangère et de sécurité des États-Unis. Internet a longtemps été présenté par la diplomatie américaine comme une infrastructure globale afin de défendre ses propres intérêts. L'instrumentalisation de son ossature – privatisée – représente désormais

46. L. Gamaury, « *Splinternet* : quand la menace d'une fragmentation d'Internet se précise », *20 Minutes*, 4 octobre 2022, disponible sur : www.20minutes.fr.
47. W. Drake, V. Cerf, W. Kleinwächter, « Internet Fragmentation: An Overview », *op. cit.*, p.50-52 et 56.

l'un des déterminants-clés de la « fragmentation » d'Internet dans les enceintes internationales dédiées.

En conservant une focale américaine, trois temps ont, historiquement, alimenté ce processus. Premièrement, dès les prémices de l'après-guerre froide, les États-Unis, dans un contexte de dérégulation destiné à fournir des opportunités de marché à leurs entreprises, diffusent le récit d'un Web naissant qui favorise l'horizontalité, sans coût d'entrée et dont l'accès ne doit en aucun cas dépendre d'une seule entreprise. De façon similaire, les ressources critiques d'Internet étaient considérées affranchies des frontières : les lois applicables aux serveurs étaient présentées par le gouvernement américain comme des incongruités. Cette approche est confirmée par le discours du vice-président Al Gore (1993-2001) à la conférence de l'Union internationale des télécomunications (UIT) à Buenos Aires en 1994[48]. Constatant la popularité de la « Déclaration d'indépendance du cyberespace » de John Perry Barlow en 1996, aux accents libertariens, la diplomatie américaine reprend le récit d'un Internet comme projet global : ce n'est pas une infrastructure américaine développée collectivement, mais une « infrastructure globale de l'information[49] ».

Le deuxième temps est marqué par l'entremêlement de deux processus convergeant vers une exploitation de l'infrastructure Internet à des fins de sécurité nationale à partir du 11 septembre 2001. D'une part, les autorités américaines permettent au marché des plateformes numériques et des fournisseurs de services de se consolider autour de quelques entreprises nationales. D'autre part, Washington repense Internet comme un outil de coercition stratégique ; un instrument *via* lequel la donnée peut soit être secrètement extraite de cibles (par le biais de programmes d'espionnage[50]) ; soit disséminée vers des cibles correspondant aux États qui cherchent à limiter les flux numériques (au moyen d'une diplomatie publique reconfigurée autour des outils numériques[51]). Imbriqués, ces processus de consolidation du marché et de surveillance accrue à la faveur de la lutte antiterroriste rationalisent les rapports entre l'appareil de renseignement américain et les sociétés privées d'Internet.

Le troisième temps correspond à la période ouverte avec la campagne présidentielle américaine en 2016, qui voit la prise de conscience occidentale d'une intensification des usages d'Internet (attaques cyber, manipulations informationnelles, etc.) par les adversaires des États-Unis. Il s'agit dès lors

48. « Inauguration of the First World Telecommunication Development Conference », discours du vice-président Al Gore, Buenos Aires, 21 mars 1994, disponible sur : https://search.itu.int (PDF).
49. « The Global Information Infrastructure », White House Forum on the Role of Science and Technology in Promoting National Security and Global Stability, 29-30 mars 1995, disponible sur : https://clintonwhitehouse4.archives.gov. Voir aussi « Global Information Infrastructure and Global Information Society », *OECD Digital Economy Papers*, n° 18, OCDE, 1996, disponible sur : www.oecd-ilibrary.org.
50. Voir E. Snowden, *Mémoires vives*, Paris, Seuil, 2019.
51. J. Nocetti, « La diplomatie d'Obama à l'épreuve du Web 2.0 », *Politique étrangère*, vol. 76, n° 1, Ifri, printemps 2011, p. 157-169.

pour Washington de bloquer ou couper l'accès des acteurs hostiles aux États-Unis à l'infrastructure critique d'Internet. Si les missions développées à partir de 2001 perdurent – et font des données la matière principale du redéploiement économique et de la stratégie de sécurité de Washington –, les États-Unis menacent dorénavant d'exclure des États d'espaces critiques d'Internet.

Le déplacement du centre de gravité démographique d'Internet vers l'Asie et l'échec relatif des États-Unis à atteindre leurs objectifs dans les enceintes de gouvernance d'Internet expliquent l'intérêt de Washington à accélérer un processus de fragmentation, afin d'assurer que les États-Unis puissent imposer les termes d'un processus de connectivité en réseau. En 2020, pendant la présidence de Donald Trump, le Clean Network Program a été pensé pour purger les réseaux des États-Unis (et ses partenaires) des applications et équipements chinois « non fiables » (TikTok, WeChat, Huawei, etc.) Le « Clean Network » devait conférer aux États-Unis les moyens de dicter les conditions d'entrée en demandant à leurs partenaires d'exclure les entreprises chinoises de l'ensemble des couches d'Internet, et notamment des infrastructures de connectivité. Cette initiative participait alors d'une fragmentation d'Internet pourtant traditionnellement critiquée par Washington. L'administration Biden, si elle n'a pas repris à son compte ce label de « Clean Network », poursuit activement la campagne contre les fournisseurs chinois, notamment Huawei, auprès de ses partenaires[52]. Plus largement, elle a fait du *friend-shoring* – faire de la fiabilité politique des partenaires un critère essentiel dans la conception des chaînes d'approvisionnement mondiales – une dimension centrale de la réorientation de sa diplomatie d'Internet autour d'un « découplage » avec la Chine.

Au-delà donc de débats internationaux qui relaient parfois le message d'une fragmentation à la faveur d'une demande d'évolution dans les processus de gouvernance d'Internet, le facteur américain ne peut être occulté dans les dynamiques de scission à l'œuvre. Il est même structurel et catalyse le discours sur la Chine. À titre d'exemple, l'annonce du retrait par Washington de ses propositions émises en 2019 à l'Organisation mondiale du commerce (OMC) – interdire aux États d'imposer des mesures de stockage ou de traitement des données sur leur sol et d'examen du code source des logiciels – a renforcé la perception d'une politique américaine d'endiguement de la stratégie numérique chinoise[53].

52. Voir M. Velliet, « Convince and Coerce: U.S. Interference in Technology Exchanges Between Its Allies and China », *Études de l'Ifri*, Ifri, février 2022, disponible sur : www.ifri.org ; J. Sakellariadis et L. Pfahler, « Transatlantic Blame Game: Trump, Merkel, Biden and the Danger of Germany's Dependence on Huawei », *Politico*, 15 octobre 2023.

53. D. Lawder, « U.S. Drops Digital Trade Demands at WTO to Allow Room for Stronger Tech Regulation », Reuters, 26 octobre 2023, disponible sur : www.reuters.com.

Une autre lecture de la fragmentation d'Internet : les initiatives de quatre acteurs

Le scénario de la fragmentation d'Internet est souvent présenté comme une opposition entre l'Occident et « le reste » – c'est-à-dire, dans la majorité des analyses, une alternative sous supervision chinoise[54]. En 2024, dépasser cette lecture binaire s'impose tant les reconfigurations dans ce domaine se révèlent profondes depuis l'intensification de la compétition technologique sino-américaine et le déclenchement de l'invasion russe de l'Ukraine. Les États-Unis, la Chine et l'Union européenne (UE) portent chacun une vision distincte du capitalisme numérique. Ces visions produisent, à des degrés très variés, des formes de « fragmentation » qu'il importe de hiérarchiser. Associer la Russie et l'Inde à cette lecture est déterminant pour comprendre les dynamiques politiques qui sous-tendent ces tendances centrifuges.

Chine : une stratégie globale de fragmentation

Les facteurs numériques et technologiques prennent une part éminente dans les ambitions internationales chinoises. La Chine se situe dans une démarche de quête de rang *via* un effort au long cours de rattrapage technologique et une volonté de briser la domination des États-Unis sur l'espace numérique.

Le pays contribue également de manière significative à la fragmentation de l'Internet global pour des raisons de politique intérieure : la « Grande muraille pare-feu » (*Great Firewall*) illustre, depuis le début des années 2000, la défense vigoureuse du contrôle d'Internet à l'échelle nationale par une censure intégrée dans l'architecture même du réseau chinois, où les principaux services des acteurs américains comme Facebook, Twitter et YouTube sont interdits depuis 2009 et Google depuis 2010.

Imposer les standards techniques du futur

La Chine a mesuré le caractère stratégique de l'élaboration et de l'imposition des normes et standards techniques liés à Internet, contribuant d'ailleurs à en

54. A. Barrinha et T. Renard, « Power and Diplomacy in the Post-Liberal Cyberspace », *International Affairs*, vol. 96, n° 3, 2020, p. 765, disponible sur : https://academic.oup.com.

faire un enjeu classique des rapports internationaux[55]. En 2018, Huawei rendait public son projet d'« infrastructure Internet décentralisée » à l'UIT, prétextant que l'Internet actuel rencontre de « sérieux problèmes » et affronte des vulnérabilités critiques liées à des attaques informatiques en hausse, à la centralisation de son architecture et à la multiplication des biais[56]. En septembre 2019 – soit au plus fort des tensions sino-américaines –, les délégations chinoises réitèrent l'initiative d'un « Internet décentralisé », qui sera nommée « New IP » lors de réunions au sein de la branche standardisation des télécommunications à l'UIT ainsi qu'en marge de sessions à l'Internet Engineering Task Force (IETF)[57]. Ladite technologie prétend remanier l'architecture technique originelle de l'Internet et le protocole TCP/IP afin de supporter la croissance des nouveaux usages (télémédecine, voiture autonome, communications holographiques, etc.). Elle intègre également un protocole d'arrêt qui permet à un acteur central d'isoler une adresse IP du reste du réseau. Les adresses mais aussi les paquets envoyés et reçus seraient reliés à l'identité du propriétaire de l'ordinateur ou du titulaire de la connexion. L'initiative suscite de vives réactions émanant des communautés multi-acteurs d'Internet, globalement favorables à une forme de *statu quo* sur le mode de gouvernance d'Internet. Elle illustre toutefois que Pékin vise à promouvoir, par la technique, une autre gouvernance d'Internet en plus d'un Internet alternatif[58]. Entre 2020 et 2022, de nombreux débats relatifs à l'interopérabilité retardent l'avancée du « New IP » à l'UIT. À partir de 2021, toutefois, les positions chinoises sur ce projet parviennent à être disséminées dans des propositions de l'enceinte onusienne[59].

Deux lectures peuvent être faites de la proposition de « New IP ». D'un côté, plutôt que de décentraliser Internet, ce projet, qui reconfigure les principes fondateurs d'Internet tels que les mécanismes de confiance (par exemple les infrastructures publiques, l'utilisation du chiffrement, etc.), les noms de domaine et les protocoles Internet, sert à légitimer le cadre plus global de la politique étrangère chinoise et, dans Internet, le modèle de gouvernance stato-centré qui la soutient[60]. Cette lecture est indissociable de craintes plus larges entourant l'exportation par la Chine de son modèle d'autoritarisme numérique[61]. D'un autre côté, certains invitent à ne pas sous-

55. J. Seaman, « China and the New Geopolitics of Technical Standardization », *Notes de l'Ifri*, janvier 2020, disponible sur : www.ifri.org.
56. Voir « Decentralized Internet Architecture », Light Reading, 20 novembre 2018, disponible sur : www.lightreading.com.
57. Le document présenté par Huawei à cette occasion, « New IP: Shaping the Future Network », est disponible sur : www.itu.int.
58. M. Murgia et A. Gross, « Inside China's Controversial Mission to Reinvent the Internet », *Financial Times*, 27 mars 2020, disponible sur : www.ft.com.
59. Voir *Global Connectivity Report 2022*, Union internationale des télécommunications, 2022, disponible sur : www.itu.int.
60. S. Hoffmann, D. Lazanski et E. Taylor, « Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet », *Journal of Cyber Policy*, vol. 5, n° 2, 2020, p. 255, disponible sur : www.tandfonline.com.
61. N. Inkster, *The Great Decoupling: China, America and the Struggle for Technological Supremacy*, Londres, Hurst, 2020, p. 157-158.

estimer les ressorts économiques derrière l'initiative de « New IP » au profit d'une lecture strictement centrée sur les capacités de contrôle et de surveillance déployées par Pékin au cœur des réseaux numériques[62].

En matière de standardisation, Huawei conserve une position tout aussi centrale dans la proposition de protocole IPv6+, présenté comme une version améliorée de l'IPv6. Conçue dès 2019, l'initiative chinoise n'est mentionnée dans les documents de l'UIT qu'à partir de 2022, où elle est présentée comme une extension naturelle de l'IPv6 plutôt que comme une architecture radicalement nouvelle[63]. Comme le « New IP », ce projet n'est pas décorrélé de ressorts commerciaux, le produit d'entreprise prenant le dessus sur le protocole technique destiné à supporter la forte croissance du nombre de terminaux connectés. L'Afrique subsaharienne ferait ainsi l'objet de convoitises en la matière, replacées dans le cadre plus large des Nouvelles routes de la soie numériques[64]. Les incertitudes pesant sur le fonctionnement de ce protocole, en particulier l'éventuelle imposition à tout le trafic Internet de données supplémentaires, attisent la perception d'une fragmentation[65].

Hardware *: des exportations tous azimuts au croisement de la géopolitique et du commerce*

La Chine accroît ses efforts d'autonomisation en matière d'équipements numériques ainsi que d'exportation de ses propres matériels informatiques. Sa stratégie repose sur un protectionnisme assumé et un soutien étatique particulièrement visible dans l'infrastructure Internet mobile (stations de base 5G), la navigation satellitaire (Beidou), les câbles sous-marins et, de plus en plus, l'Internet satellitaire.

Les efforts de Pékin pour sécuriser ses chaînes d'approvisionnement – ajoutés aux réponses occidentales que les autorités politiques perçoivent comme un facteur de risque supplémentaire – sont susceptibles d'alimenter une fragmentation commerciale et juridique d'applications de *hardware* avant de conduire à une fragmentation technologique bien réelle, différents standards techniques de *hardware* coexistant à l'échelle globale[66]. La révision d'un cadre législatif sur la cybersécurité (2013 puis 2017) a

62. A. Mueller et C. S. Yoo, « Crouching Tiger, Hidden Agenda? The Emergence of China in the Global Internet Standard-Setting Arena », *Research Paper* n° 23-33, University of Pennsylvania, Institute for Law and Economics, août 2023, disponible sur : https://papers.ssrn.com.
63. L. Bertuzzi, « La Chine modifie sa proposition sur la gouvernance d'Internet et cible les pays en développement », Euractiv, 7 juin 2022, disponible sur : www.euractiv.fr.
64. H. Tugendhat et J. Voo, « China's Digital Silk Road in Africa and the Future of Internet Governance », *Working Paper*, n° 50, China-Africa Research Initiative, School of Advanced International Studies (SAIS), Johns Hopkins University, 2021, disponible sur : www.econstor.eu.
65. L. Bertuzzi, « La Chine modifie sa proposition sur la gouvernance d'Internet et cible les pays en développement », *op. cit.*
66. K. von Carnap, A. Hmaidi, R. Arcesati et J. Groenewegen-Lau, « Fragmenting Cyberspace: The Future of the Internet in China », *MERICS Report*, MERICS, novembre 2023, p. 48, disponible sur : https://blog.merics.org.

considérablement restreint la marge de manœuvre des équipementiers étrangers en Chine[67].

Les succès des équipementiers chinois à l'export favorisent la diffusion d'une fragmentation commerciale et juridique à l'échelle globale. Les projets chinois sont noués le plus souvent *via* des accords bilatéraux qui placent les contractants dans une situation de dépendance technologique et financière de long terme, susceptible d'attiser la logique de « découplage[68] ». L'effet miroir avec les critères et la tonalité du programme américain « Clean Network » est palpable[69].

Pékin considère l'infrastructure d'Internet comme un ensemble stratégique dans lequel les acteurs nationaux doivent prendre leur part. Huawei – bien que de façon moindre depuis les sanctions américaines la visant – ou HMN (Huawei Marine Networks, filiale du groupe Hengtong), un câblier bénéficiant d'une intégration verticale (il est aussi opérateur), reçoivent un soutien étatique significatif leur permettant de renforcer leurs parts de marché. HMN a déployé le câble *Pakistan & East Africa Connecting Europe* (PEACE) – composante des Nouvelles routes de la soie qui relie les côtes pakistanaises et françaises *via* le Kenya – et, en Europe, a tiré les câbles *Silphium* entre la Grèce et la Libye et *Hannibal* entre la Sicile et l'Algérie[70]. Depuis 2022, toutefois, les pressions américaines visant les projets de câbles incluant une ou plusieurs parties prenantes chinoises (même sans participation d'entreprises américaines) ont abouti soit au gel des projets, soit à l'exclusion des câbliers chinois. Ainsi en a-t-il été du projet de câble *Cap-1* devant relier la Californie à Singapour *via* Hong-Kong et la Malaisie (avorté) ; du projet *Sea-Me-We 6* entre Singapour et Marseille, accordé à l'américain SubCom et non à HMN ; ou encore des câbles *Medusa* (connectant l'Égypte au Portugal) et *Africa-1* (reliant le Kenya à la France), attribués au français ASN et non à HMN qui avait pourtant été invité à candidater[71].

Applications : WeChat et la logique de couches de fragmentation

Avec TikTok, WeChat représente le succès le plus notable de l'économie numérique chinoise et de son exportation au-delà des frontières du pays. Les caractéristiques techniques de cette « super-application » (constituées de mini-programmes qui sont autant d'univers applicatifs) brident

67. Voir N. Alsabah, « China's Cyber Regulations: A Headache for Foreign Companies », *Comment*, MERICS, 22 mars 2017, disponible sur: https://merics.org.
68. N. Inkster, *The Great Decoupling*, *op. cit.*
69. Voir M. Rithmire, C. Han, « The Clean Network and the Future of Global Technology Competition », Harvard Business School, *HBS Case 721-045*, 12 avril 2021, disponible sur : https://globaltechsecurity.com.
70. J. Brock, « U.S. and China Wage War Beneath the Waves – Over Internet Cables », Reuters, Special Report, 24 mars 2023, disponible sur : www.reuters.com. Voir aussi D. Aluf, « China's Subsea-Cable Power Play in the Middle East and North Africa », Atlantic Council, *Issue Brief*, mai 2023, disponible sur : www.atlanticcouncil.org.
71. A. Gross, A. Heal, C. Campbell *et. al.*, « How the U.S. Is Pushing China Out of the Internet's Plumbing », *Financial Times*, 13 juin 2023, disponible sur : https://ig.ft.com/subsea-cables.

l'interconnectivité entre les différentes parties du réseau, conduisant à une fragmentation technique. La plateforme s'apparente aujourd'hui davantage à un nouveau type d'infrastructure bâtissant des « jardins clôturés » les uns dans les autres, à la manière de poupées gigognes[72]. En effet, les programmeurs qui développent des applications pour l'infrastructure des mini-programmes doivent utiliser le langage de script propriétaire de WeChat, seulement accessible *via* l'interface de l'application. En comparaison d'acteurs comme Apple, également parties prenantes de la création de « *walled gardens* », WeChat produit de multiples couches de fragmentation : la compatibilité entre smartphones par rapport aux mini-programmes de l'application ; un processus d'enregistrement restrictif ; des caractéristiques segmentées par la géolocalisation[73].

Ces trois cas d'étude ne présentent aucun caractère d'exhaustivité tant la fragmentation consécutive aux politiques numériques chinoises s'est diversifiée. Mentionnons une tendance de fond qui voit les autorités chinoises viser l'extraterritorialité de ses lois en matière de gouvernance des données (leur collecte, traitement et transfert, ainsi que leur commerce), dans une double optique politique (remettre en cause l'hégémonie perçue du droit américain, défendre une approche spécifique de la souveraineté des données) et économique (soutenir le déploiement des Nouvelles routes de la soie numériques[74]).

Russie : en marche vers une scission de l'Internet mondial

L'approche politique des autorités russes à l'égard d'Internet articule étroitement les dimensions intérieure et extérieure. Les déclarations publiques des décideurs et la fabrique de la loi s'imbriquent dans des initiatives politiques régionales et internationales, tandis que les événements globaux influencent en retour la politique numérique de la Russie[75]. Le maître-mot de la politique numérique russe est celui de souveraineté, laquelle doit s'appréhender sous les angles stratégique, informationnel et économique : la politique russe dans ce domaine est déterminée par l'hostilité aux États-Unis, et le Kremlin souhaite atténuer la dépendance du pays à l'égard des principales plateformes américaines.

72. J.-C. Plantin et G. de Seta, « WeChat As Infrastructure: The Techno-Nationalist Shaping of Chinese Digital Platforms », *Chinese Journal of Communications*, vol. 12, n° 3, 2019, disponible sur : www.tandfonline.com.
73. K. von Carnap *et al.*, « Fragmenting Cyberspace: The Future of the Internet in China », *op. cit.*, p. 33.
74. W. Cong, « The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics », *in* L. Belli et M. Jiang (dir.), *Digital Sovereignty in the BRICS Countries*, Cambridge, Cambridge University Press, à paraître en 2024.
75. J. Nocetti, « Contest and Conquest: Russia and Global Internet Governance », *International Affairs*, vol. 91, n° 1, 2015, p. 115.

La quête d'une indépendance numérique

L'approche fondamentalement légaliste portée par les autorités russes dans la sphère numérique a trouvé son aboutissement en 2019 avec la loi dite « pour un Internet souverain ». L'idée-force de cette loi est de permettre à la Russie de se doter d'un poste de commandement unique, à partir duquel les autorités pourraient gérer les flux d'informations dans le cyberespace russe ; cela inclut la surveillance, la limitation ou le blocage de ces flux sur tout ou partie de l'étendue de l'Internet russe. Les dispositions de la loi portent en priorité sur deux aspects : le routage du trafic Internet et le contrôle du système de noms de domaine[76].

Le second point est en réalité le résultat d'un processus entamé depuis une décennie. En envisageant la création d'un système de noms de domaine « national », les autorités conçoivent un dispositif qui doit permettre à Internet de continuer à fonctionner même en cas de scission avec l'Internet mondial. Depuis 2015, deux processus se sont matérialisés ; d'une part, la reprise en main des organismes de coordination du DNS (registraire et registre, ou *registrar* et *registry* en anglais), jusqu'alors refuges des pionniers de l'Internet russe. D'autre part, une série de tests conduits à haut niveau de l'État visaient à s'assurer de la résilience du RuNet si un *shutdown* numérique était décidé par le Kremlin en cas de crise – intérieure (par le fait d'un militantisme numérique trouvant un débouché dans la rue) ou extérieure (dans le cas de cyberattaques ciblant la Russie).

Le premier dispositif consiste à réorienter les flux de données vers des points de routage maîtrisés par des acteurs contrôlés par l'État[77]. Ceux-ci filtrent le trafic Internet afin que seules les données échangées entre individus localisés en Russie parviennent à leur destination. D'un point de vue technique, la totalité du trafic en Russie doit circuler par des points d'échange Internet (IXP) approuvés au préalable par le gouvernement.

Outre le filtrage du réseau à des fins de surveillance, cette stratégie intègre la perspective d'une déconnexion d'Internet en cas de menaces extérieures. L'État a déjà montré que ce dispositif fonctionne : à l'automne 2018, à la suite de manifestations dans la république caucasienne d'Ingouchie, portant sur la révision du tracé de la frontière avec la Tchétchénie voisine, le FSB local a exigé des opérateurs locaux qu'ils coupent l'accès aux réseaux mobiles sur le territoire de la République tchétchène pendant deux semaines[78]. Le Kremlin escompte de la loi qu'elle lui permette de déployer des tactiques similaires à distance, en donnant à un centre de

76. J. Nocetti, « Russie : un horizon étroit et incertain », *in* A. Pannier (dir.), « Les politiques technologiques des puissances numériques moyennes », *op. cit.*, p. 91.
77. K. Limonier, « Vers un 'Runet souverain' ? [...] », *op. cit.*, p. 45.
78. M. Kolomychenko, « Russia Stifled Mobile Network During Protests: Document », Reuters, 16 novembre 2018, disponible sur : www.reuters.com.

commandement à Moscou le contrôle sur l'équipement qui doit être installé sur tous les fournisseurs d'accès, IXP et points de contrôle aux frontières[79].

Cependant, le caractère fortement distribué des routes d'Internet russe limite *a priori* la mise en place effective d'un « Internet souverain », particulièrement dans la perspective de déconnexion totale[80]. Il s'agit pourtant d'une démarche de scission avec le reste du réseau mondial, en raison du degré d'interdépendance de ce dernier au-delà des frontières nationales, et à tous les niveaux de protocoles.

Guerre en Ukraine et fragmentation

L'invasion russe de l'Ukraine a réveillé le spectre d'une fragmentation accélérée d'Internet (et de l'ensemble du champ technologique qui sous-tend l'économie numérique). Celle-ci s'est manifestée de plusieurs façons et sur l'ensemble des couches d'Internet. En réponse aux premiers jeux de sanctions occidentales, qui visaient à couper la Russie des principaux circuits mondiaux d'approvisionnement technologique, la Russie a interdit aux grandes plateformes technologiques américaines d'opérer sur son territoire avant de lancer (ou relancer) des alternatives russes à Google Play ou Instagram. Cette fragmentation délibérée a également été à l'initiative d'entités occidentales : ainsi le navigateur Firefox a-t-il exclu le russe Yandex de ses choix de moteur de recherche, et les « Big Tech » ont-ils déployé de vastes efforts de remédiation technique et de soutien à la lutte contre la désinformation russe au profit de l'Ukraine.

Sur la couche logique, l'invasion de l'Ukraine par Moscou s'est accompagnée d'un re-routage systématique des réseaux Internet dans les régions envahies, en obligeant ces flux à passer par la Russie. Cette réorientation des données n'a pas eu que des effets de retardement de l'acheminement mais aussi de contrôle et de filtrage de l'information, les régions ukrainiennes conquises voyant désormais le monde à travers le prisme déformé de la censure russe[81]. L'articulation entre la matérialité d'Internet et la circulation de l'information produite est ici totale, donnant corps à l'idée d'annexion numérique de territoires – qui n'est cependant qu'une des facettes des méthodes destinées à légitimer l'occupation russe en Ukraine[82].

Enfin, au début de l'invasion russe, des personnalités ukrainiennes et occidentales ont proposé à l'ICANN d'obtenir le retrait ou le blocage des adresses Internet attribuées à la Russie. Parmi les incitations faites, la

79. J. Nocetti, « Le contrôle par la loi : les autorités russes et Internet », in S. Taillat, A. Cattaruzza, D. Danet (dir.), *La Cyberdéfense. Politique de l'espace numérique* (2e édition), Paris, Armand Colin, p. 220-222.
80. K. Limonier, « Vers un 'Runet souverain' ? [...] », *op. cit.*, p. 46.
81. M. Burgess, « Russia Is Taking Over Ukraine's Internet », Wired, 15 juin 2022, disponible sur : www.wired.co.uk
82. A. Satariano et S. Reinhard, « How Russia Took Over Ukraine's Internet in Occupied Territories », *New York Times*, 9 août 2022, disponible sur : www.nytimes.com.

révocation temporaire ou définitive du TLD .ru, son équivalent en cyrillique (.рф) et le .su ; le retrait de certificats d'authentification des sites Web utilisant ces noms de domaine ; ou encore le verrouillage des serveurs racines localisés en Russie[83]. Alors président de l'ICANN, Göran Marby a rejeté la requête au motif qu'Internet reste un système décentralisé et « qu'aucun acteur n'a la capacité de le contrôler ou de le fermer », le rôle de l'ICANN « ne s'étendant pas à la prise de sanctions ou à la restriction d'accès contre des segments de l'Internet, quelles que soient les provocations[84] ».

Inde : une fragmentation partielle ?

Les récents remous dans le système international – rivalité sino-américaine, perturbation globale des chaînes d'approvisionnement commerciales et technologiques, guerre en Ukraine – ont ravivé l'ambivalence du positionnement diplomatique de l'Inde, entre « cible » de la compétition entre Washington et Pékin et acteur en voie d'autonomisation accélérée[85]. Cette ambivalence se reflète dans la posture indienne face aux enjeux de fragmentation d'Internet.

Industrie numérique, données : à la recherche d'une souveraineté

Si l'Inde est aujourd'hui très dépendante des États-Unis et de la Chine en matière d'équipements, de logiciels et de plateformes, la souveraineté numérique reste un objectif revendiqué du gouvernement et constitue un pilier de sa stratégie sur les questions numériques, dans l'esprit du slogan du Premier ministre Modi (*Atmanirbhar Bharat* – « Inde autosuffisante »[86]).

En matière de e-gouvernement, le principal projet, *India Stack*, consiste en un ensemble d'interfaces *open source* créées par l'État et réutilisables par les entreprises afin qu'elles développent des services numériques. La plus connue de ces briques, le système *Aadhar*, fournit un numéro unique d'identification à chaque Indien. Mais l'*India Stack* regroupe également une solution de vérification de l'identité (eKYC) ou un système de paiement (UPI), qui a fortement contribué au développement du secteur des FinTech[87]. Ces deux projets, s'ils ne « fragmentent » pas l'Internet global,

83. Échanges de l'auteur avec deux experts mobilisés dans cette demande adressée à l'ICANN, février-mars 2022.
84. G. Marby, Lettre au ministre ukrainien de la Transformation numérique Mykhailo Federov, ICANN, 2 mars 2022, disponible sur : www.icann.org.
85. T. Ray, « Inde : un acteur pivot », *in* A. Pannier (dir.), « Les politiques technologiques des puissances numériques moyennes », *op. cit.*, p. 31, disponible sur : www.ifri.org.
86. A. Basu, « Sovereignty in a Datafied World », ORF, *Issue Briefs*, 18 octobre 2021, disponible sur : www.orfonline.org.
87. Sur l'UPI, voir V. Hariharan et S. Natarajan, « Digital Sovereignty and Payments: A Case Study of the National Payments Corporation of India », *in* L. Belli et M. Jiang (dir.), *Digital Sovereignty in the BRICS Countries, op. cit.*

sont cependant partie intégrante d'une approche plus souveraine du champ numérique national.

En dépit d'interdépendances technologiques avec les États-Unis – l'Inde est devenue une « superpuissance de la sous-traitance informatique[88] » –, New Delhi s'oppose aux initiatives qui vont dans le sens d'une libéralisation générale des transferts de données, tout particulièrement à l'OMC. Plusieurs textes viennent imposer le stockage et le traitement sur le territoire indien de certaines données. La circulaire sur la localisation des données de la Banque de réserve indienne prévoit ainsi que toutes les données liées aux systèmes de paiements doivent être stockées dans des serveurs situés en Inde. Le projet de loi sur la protection des données prévoit de systématiser cette obligation de localisation pour toutes les données sensibles et critiques[89]. Il convient de préciser que l'approche indienne en matière de protection et de localisation des données reste motivée par des objectifs économiques davantage que stratégiques – les critères de développement du pays revêtant une dimension centrale dans les discours politiques[90].

Des relations complexes avec la tech américaine et chinoise

La politique réglementaire de New Delhi provoque des conflits récurrents avec les plateformes du numérique américaines, notamment au sujet de l'accès aux données chiffrées, de la modération des contenus et de l'environnement des affaires. Le code éthique des médias numérique de 2021 impose ainsi aux plateformes d'être en mesure de tracer l'origine des messages et de filtrer leur contenu. Ceci remet en question le modèle de chiffrement de bout en bout mis en œuvre par une société telle que WhatsApp, qui a porté le texte devant la Haute cour de Delhi en 2021[91]. Des conflits se sont également fait jour autour de la question de la régulation des contenus. En 2021 toujours, l'État indien a demandé à Twitter le blocage de certains comptes en lien avec les manifestations de paysans. Selon le gouvernement, ces comptes se rendaient coupables de « diffusion de fausses informations » menaçant « la sécurité nationale » mais l'entreprise a opposé un refus[92]. En rétribution, de nombreux représentants officiels et cadres du parti majoritaire BJP ont abandonné Twitter pour utiliser Koo, une plateforme autochtone concurrente.

88. Entretien de l'auteur, Paris, décembre 2023.
89. N. Mishra, « Digital Governance and Digital Trade in India: Losing Sight of the Forest for the Trees? », *in* A. Chander et H. Sun (dir.), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford, Oxford University Press, 2023, p. 249-253.
90. *Ibid*., p. 263.
91. Voir T. Derivry, « La souveraineté numérique en Inde : programme politique, discours, pouvoir et capacité d'action », Sciences Po, chaire Digital, gouvernance et souveraineté, 9 mai 2023, disponible sur : www.sciencespo.fr.
92. S. Phartiyal, « India to Twitter: Comply with IT Rules or Face 'Unintended Consequences' », Reuters, 5 juin 2021, disponible sur : www.reuters.com.

Ces conflits avec les Big Tech américains ont parfois des conséquences sur les relations interétatiques. Le projet indien de taxe sur les services numériques avait été identifié par la Maison-Blanche comme une discrimination à l'encontre des entreprises américaines – avant de trouver une issue favorable après des consultations bilatérales[93].

Depuis la crise ouverte entre Pékin et New Delhi en mai 2020, les autorités indiennes ont bloqué 59 applications chinoises au motif de risques pour la sécurité nationale. La liste a été progressivement élargie pour en contenir plus de 200, dont WeChat, AliExpress ou TikTok. Dans le secteur des télécommunications, Huawei et ZTE ont été exclus des phases de tests pour les réseaux 5G. Les fabricants chinois de smartphones, enfin, se sont vus imposer de fournir une liste des composants de leurs produits et des données qu'ils stockent. Ces actions ont pour conséquence de limiter fortement les possibilités d'expansion des entreprises chinoises sur le marché indien.

Une ambivalence dans les négociations internationales

Le positionnement de l'Inde dans les enceintes de gouvernance d'Internet reflète les contradictions de certains pays tentés d'esquisser une « troisième voie » entre un modèle multi-acteurs, parfois critiqué pour son manque de légitimité et de représentativité, et un modèle multilatéral de type onusien, basé sur les souverainetés étatiques. New Delhi maintient en effet une attitude fluctuante sur les moyens permettant de mêler un accroissement de la connectivité tout en bâtissant une souveraineté numérique[94]. Si le discours politique indien marque un attachement au cadre rhétorique des BRICS, avec un accent post-colonial plus tangible que chez les autres pays membres de ce forum, l'Inde se distingue des autres grands émergents par une proximité économique et sécuritaire avec les États-Unis. L'imbrication du tissu technologique indien avec l'écosystème de la Silicon Valley confère un poids politique non négligeable aux grands acteurs privés indiens (Infosys, Wipro, etc.). Ajoutée aux aspirations d'une partie substantielle de la jeunesse connectée du pays, peu de lisibilité est offerte aux positions défendues par Delhi dans les enceintes comme l'Internet Governance Forum (IGF), le comité des gouvernements (GAC) de l'ICANN, l'Open-Ended Working Group à l'Organisation des Nations unies (ONU), ou des événements comme le NETmundial de Sao Paulo en 2014[95].

93. « USTR Welcomes Agreement with India on Digital Services Taxes », Office of the United States Trade Representative, 24 novembre 2021, disponible sur : https://ustr.gov.
94. J. Nocetti, « Puissances émergentes et internet : vers une troisième voie ? », *op. cit.*, p. 50.
95. *Ibid*. Voir aussi A. Barrinha et R. Turner, « Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia, and India », *Contemporary Security Policy*, octobre 2023 (en ligne), p. 17, disponible sur : www.tandfonline.com ; M. Kaul, « Global Internet Governance: India's Search for a New Paradigm », ORF, *ORF Issue Brief*, n° 74, août 2014, disponible sur : www.orfonline.org.

Union européenne : la quête d'une « souveraineté numérique » sans fragmentation d'Internet

La fragmentation d'Internet reste peu débattue au sein de l'UE, devenue le premier émetteur de normes juridiques qui entend donner un cadre de portée mondiale à une économie numérique dominée par le duopole sino-américain. L'essentiel des débats est resitué dans une double perspective économique et juridique, fondement des ambitions européennes de « souveraineté numérique ».

Le droit plus fort que la « fragmentation » ?

Dans un contexte de durcissement des rapports dans l'espace numérique international, l'UE s'est jusqu'à présent distinguée par sa qualité de « superpuissance réglementaire[96] ». Cette préférence pour agir par la norme sur la scène internationale ne constitue pas une donnée inédite de la politique européenne : celle-ci renforce ce qui demeure sa ressource (géo)politique majeure, à savoir une capacité à produire et à déployer à l'échelle mondiale un large dispositif de normes[97]. Dans le domaine numérique, cet « effet Bruxelles » décrit, selon Anu Bradford, la capacité de l'UE à étendre son influence sur les marchés internationaux en tirant profit de sa puissance normative pour façonner les politiques des données personnelles des plateformes technologiques extra-européennes et des États[98].

Cette stratégie normative de l'UE dans le numérique se fonde sur une ambition juridique incontestable, avec la mobilisation d'outils d'extraterritorialité. À partir de 2020, s'ouvre une période marquée par une profusion de publications institutionnelles et juridiques : *Livre blanc sur l'intelligence artificielle* (février 2020), « Boussole numérique » (juin 2021), « Boîte à outils » sur la 5G (2020), Stratégie pour la donnée, *Digital Markets Act* et *Digital Services Act* (2023), Plan d'action pour l'éducation numérique 2021-2027, Plan d'action pour les technologies financières, *Cybersecurity Act*, *AI Act*, « Bac à sable » réglementaire sur les *blockchains*, etc. Précisons que certains de ces textes, comme celui sur la 5G, ne revêtent aucun caractère contraignant.

L'UE atteste donc un puissant tropisme juridique avec l'utilisation du droit du marché intérieur et la sollicitation des principes et des valeurs inscrites dans les traités européens. Pour Bruxelles, l'enjeu est de transcrire juridiquement les ambitions politiques, avec l'idée-force, depuis 2019, de

96. A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford, Oxford University Press, 2020.
97. *Ibid.*
98. A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, Oxford, Oxford University Press, 2023, p. 324-326.

présenter un grand texte européen (« *Act* ») par grand enjeu numérique et d'avoir ainsi une loi européenne identifiable dans le monde entier, en assumant l'extraterritorialité de ses législations[99].

L'UE paraît donc amorcer les contours d'une diplomatie du numérique qui ne dissimule pas une forme d'unilatéralisme, en jouant sur l'effet d'entraînement de la régulation européenne au niveau global. Le Pacte numérique mondial, initiative des Nations unies censée définir les principes communs du futur de l'Internet qui sera discuté en septembre 2024, a fait l'objet d'une communication du Conseil de l'UE portant partiellement sur la nécessité d'éviter une fragmentation technique, économique et géopolitique d'Internet[100].

Vers une autonomie stratégique par les infrastructures ? Le projet DNS4EU

Mentionné dans la stratégie de cybersécurité de l'UE pour la décennie numérique[101], le projet de résolveur DNS européen a été formellement lancé en janvier 2022. Il existe deux catégories de serveurs DNS : le serveur faisant autorité, qui stocke les données, récupérées *via* le protocole DNS ; et le résolveur, qui correspond au serveur qu'interrogent directement les terminaux. L'initiative DNS4EU vise à répondre tant à la consolidation exponentielle du marché des résolveurs DNS qu'à la prolifération des risques numériques (cyberattaques, pannes). Sur le plan industriel, les acteurs extra-européens (Google, Cloudflare) dominent en effet le marché des résolveurs dits ouverts[102].

Sur le plan technique, le DNS4EU devra se conformer aux dispositions juridiques existantes, notamment en matière de filtrage obligatoire des adresses Web renvoyant à des contenus illicites (apologie du terrorisme, pédopornographie, sites de piratage, etc.). Le DNS4EU répond à un objectif d'accessibilité au plus grand nombre et de compatibilité maximale entre terminaux et systèmes d'exploitation, notamment sur les normes de sécurité et de respect de la vie privée, ainsi qu'avec le protocole IPv6. Pas vers la construction d'une « autonomie stratégique » européenne sur le plan technologique, le DNS4EU constitue par ailleurs l'intervention de Bruxelles la plus notable dans un marché largement privatisé reposant sur le libre arbitre des consommateurs[103]. Si le projet n'a, depuis, pas connu de

99. B. Bertrand (dir.), *La Politique européenne du numérique*, Bruxelles, Bruylant, 2022.
100. « European Union Contribution to the Global Digital Compact », mars 2023, disponible sur : www.un.org.
101. « The EU's Cybersecurity Strategy for the Digital Decade », Commission européenne, 14 décembre 2020, disponible sur : https://digital-strategy.ec.europa.eu.
102. Vingt pourcents du trafic Internet mondial dépend de résolveurs ouverts. Voir A. Durand, « DNS Resolvers Used in the EU », ICANN, 1er mars 2022, disponible sur : www.icann.org.
103. R. Radu, « DNS4EU: A Step Change in the EU's Strategic Autonomy? », *Journal of Cyber Policy* (en ligne), décembre 2023, disponible sur : www.tandfonline.com.

phase de développement notable, le déploiement du DNS4EU est censé intervenir fin 2025.

Répondre à l'équation marché-sécurité pour le DSN4EU, comme l'explicite la stratégie de cybersécurité de l'UE, répond en substance à d'autres documents rendus publics par les institutions européennes, telle que la Directive sur la résilience des entités critiques et la Directive NIS-2.

L'action de l'UE pour l'infrastructure Internet présente également un volet diplomatique. L'initiative « Portail mondial » (*Global Gateway*) présentée en décembre 2021 par la Commission européenne, consiste en une série d'engagements à investir dans les infrastructures dites de connectivité – de façon analogue au projet chinois des Nouvelles routes de la soie –, y compris dans les infrastructures numériques telles que les câbles sous-marins et terrestres à fibre optique, les systèmes de communication satellitaires sécurisés et les infrastructures *cloud*. Dans ce contexte, les investissements de l'UE seront liés aux « normes et protocoles qui soutiennent la sécurité et la résilience des réseaux, l'interopérabilité et un internet ouvert, pluriel et sécurisé[104] ». Ce faisant, l'UE mène une politique qui vise précisément à contrer la tendance mondiale à la fragmentation.

104. « La stratégie Global Gateway », Communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen, au Comité des régions et à la Banque européenne d'investissement, Commission européenne, 1er décembre 2021, disponible sur : https://eur-lex.europa.eu.

Conclusion

Alors que la continuité d'Internet garantissait une forme de dissuasion originelle – l'interdépendance et la connexion à un même réseau étant gages de vulnérabilité mutuelle –, sa compartimentation actuelle en réseaux « nationaux » par les États autoritaires est susceptible d'accroître davantage l'instabilité dans le cyberespace. La tentation pour ces derniers de s'en prendre directement à leurs adversaires sera proportionnelle à leur capacité à préserver leur réseau de répercussions accidentelles[105] ou de représailles.

La concentration du trafic des données autour de quelques acteurs centraux du routage (GAFAM notamment) crée elle aussi des risques en matière de continuité globale des services Web, comme l'a montré la panne géante de Facebook. En octobre 2021, le réseau social et ses filiales (dont WhatsApp et Instagram) ont été frappés d'une panne ressentie mondialement pendant plus de sept heures, causée par la perte de routes IP vers les serveurs DNS de Facebook. Tout en incitant ces *gatekeepers* à davantage de responsabilité, il s'agit de soutenir la déconcentration et la diversification globale du routage. Cette composante « commerciale » de la fragmentation nécessite une prise en compte plus soutenue en dépit de l'emphase plus souvent placée sur les intentions géopolitiques des États.

À ce titre, tant l'approche duale de la Chine en matière de développement de standards Internet (qui combine coopération et fragmentation) que l'ambition de la Russie de reconcevoir son infrastructure Internet, ou l'apparente ambivalence de l'Inde, illustrent la façon dont les États adoptent des approches de plus en plus stratégiques vis-à-vis d'Internet et de ses normes. L'UE, par son positionnement spécifique fait de construction patiente d'un consensus et de pari sur l'exportation de son droit, se distingue de ces trois pays en résistant aux forces centrifuges traversant le champ numérique. Les États-Unis, quant à eux, attachés au maintien de leur primauté technologique – à commencer par l'édifice Internet – ajustent leur posture traditionnelle liant ouverture technologique, innovation et démocratisation des sociétés, pour afficher désormais une politique plus coercitive et sino-centrée.

La notion de fragmentation présente ainsi l'intérêt de mettre en lumière des phénomènes de première importance dans le champ numérique, qui se répercutent concrètement pour les usagers. Elle n'est toutefois pas exempte d'ambiguïtés : le terme a pu être employé à tout propos dans les discours politiques, du système de noms de domaine à la neutralité du net, jusqu'à la

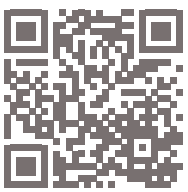
105. À la manière de la cyberattaque NotPetya de 2017, lancée par des opérateurs russes contre les réseaux ukrainiens, et dont la diffusion incontrôlée a fini par affecter des systèmes informatiques en Russie.

censure en ligne et aux différents régimes de respect de la vie privée, prêtant ainsi à confusion, notamment aux États-Unis.

Les nuances du capitalisme numérique interrogent la coexistence des différents modèles : « l'Internet ouvert » de la Silicon Valley, « l'Internet commercial » de Washington, « l'Internet paternaliste » chinois et « l'Internet bourgeois » de Bruxelles[106] présentent tous des spécificités philosophiques, juridiques et économiques bien marquées. Socle ou miroir d'un système international déjà fragmenté, Internet affronte le risque d'une instabilité permanente qu'il faudra néanmoins maîtriser en préservant ses acquis.

Symbolique des débats relatifs à Internet pendant la décennie 2010, la fragmentation était alors discourue principalement dans des cénacles d'experts. Elle était aussi majoritairement focalisée sur les risques propres au DNS. Depuis, la profusion d'enjeux de nature géopolitique et commerciale, notamment, a donné un caractère plus tangible voire systémique aux perspectives de fragmentation, que l'enjeu du « découplage » technologique sino-américain vient questionner frontalement.

106. C'est la taxonomie retenue par K. O'Hara et W. Hall dans *The Four Internets: Data, Geopolitics, and the Governance of Cyberspace*, Oxford, Oxford University Press, 2021.



27 rue de la Procession 75740 Paris cedex 15 – France

Ifri.org