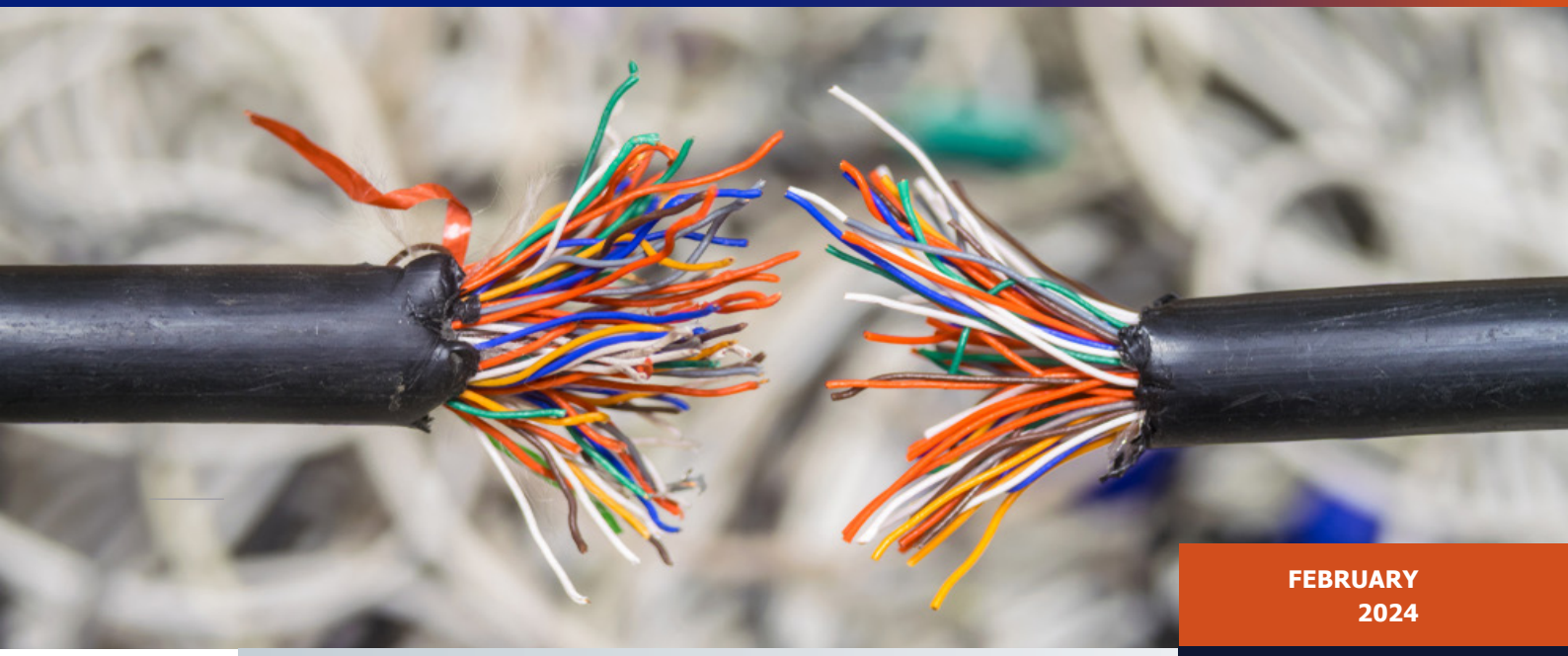
IFRI
STUDIES

GEOPOLITICS OF TECHNOLOGY CENTER



FEBRUARY
2024

A Splintered Internet?
Internet Fragmentation and the Strategies of China, Russia, India and the European Union

Julien NOCETTI

The French Institute of International Relations (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit foundation according to the decree of November 16, 2022. As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience.

Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

ISBN: 979-10-373-0882-5

How to cite this publication:
Julien Nocetti, "A Splintered Internet? Internet Fragmentation and the Strategies of China, Russia, India and the European Union", *Études de l'Ifri*, Ifri, February 2024.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

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

Email: accueil@ifri.org

Website: Ifri.org

Author

Julien Nocetti is an Associate Research Fellow at the French Institute of International Relations (Ifri) and a member of the GEODE center (Geopolitics of the Datasphere) at Université Paris 8. He holds a PhD in political science and was a research fellow at Ifri from 2009 to September 2019, before becoming an associate professor at the Saint-Cyr Coëtquidan military academy from 2019 to 2023. He is a member of the editorial board of the journal *Intelligence and Cyber French Studies* and of the CIGREF strategic orientation council. His research focuses, firstly, on global digital issues (digital and artificial intelligence diplomacy, cyber-conflict) and, secondly, on Russian foreign policy, in particular its digital and cyber strategies. He recently coordinated a special issue of the journal *Annales des Mines – Enjeux numériques* dedicated to digital sovereignty (No. 23, September 2023).

Executive Summary

From the Covid-19 pandemic to the ramifications of Russia's full-scale 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 domestic and foreign policies, are likely to accelerate this fragmentation, whether voluntarily or not. The role of private companies, 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 which, 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 a variety of practices: data localization, deliberate Internet shutdowns, policies aimed at excluding Chinese companies from all Internet layers, and, in particular, 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 main gateway to the global Internet.

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 key determinants of the dynamics of "fragmentation". The study then examines the policies pursued by China, Russia, India, and the European Union, whose initiatives are driven by very diverse goals and are also reconfiguring the Internet. Indeed, these initiatives are manifold, reflecting the distinct visions of digital capitalism held by these state actors.

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.

Table of contents

Introduction

In a July 2022 report, the Council on Foreign Relations (CFR) task force examining the future of American Internet diplomacy delivered a stark assessment of the shortcomings of Washington's policies in this area. “The era of the global Internet is over” the report begins, and goes on to say that the Internet is now “more fragmented, less free and more dangerous” than it was a decade ago[1]. Whether this reflects a passing worry or deep-seated concerns, it is worth examining how the major powers influence the global Internet ecosystem, through their domestic and foreign policies.

A recurrent theme in debates surrounding the Internet for nearly two decades, and more recently in the digital and technological fields, “fragmentation” results from the Internet's compartmentalization, reflecting its gradual territorialization by states. This development seems to contradict the Internet's historic identity – an open, neutral and unbroken space which, as its founders envisioned it, was founded on the principles of decentralization, anonymity, accessibility and equality between users.[2]

We must first distinguish between the Internet (the infrastructure, i.e. the network of networks) and the Web (its application layer, where Internet consumers go), for which the principles of fragmentation differ. In some countries (China, Russia, Iran, North Korea, Cambodia, Myanmar, etc.), partial or complete state control of the Internet tends to undermine its continuity and greatly increases the risks for the affected populations: political repression, attacks on human rights and privacy. While some call for the global network to be more evenly structured, given the United States' historical dominance, authoritarian states are more interested in gaining physical control over a space that could escape their reach, and from which domestic and/or external threats may arise.

This network fragmentation coincides with the Web's fragmentation, with users navigating between a range of more or less heterogeneous spaces. In order to overcome algorithmic enclosures (which promote the spread of fake news and information bubbles) that isolate Internet users from each other, data portability, transparency and service interoperability are essential prerequisites for an open Web that ensures global connectivity.

---

1. N. Fick and J. Miscik (ed.), “Confronting Reality in Cyberspace. Foreign Policy for a Fragmented Internet”, *Independent Task Force Report*, no. 80, Council on Foreign Relations, July 2022, p. 7, available at: www.cfr.org.

2. Read for example F. Turner, *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*, Chicago: University of Chicago Press, 2008; and B. Loveluck, *Réseaux, libertés et contrôle. Une généalogie politique d’internet*, Paris: Armand Colin, coll. Le Temps des idées, 2015.

This fragmentation is, therefore, already a reality and affects different spaces, with varying interpretations depending on the parties in question. Regardless, any analysis of the Internet's fragmentation must consider the national interests that run throughout the digital arena, epitomized by the "digital sovereignty" that many international actors so fervently seek.[3]

From the Covid-19 pandemic to the consequences of Russia's invasion of Ukraine, current events are rich with examples of this growing fragmentation. The transatlantic dispute over data transfers, China's efforts to set its own Internet standards, speculation over a potential ban of the Chinese social network TikTok in the U.S., and the investment strategies of major U.S. and Chinese digital actors all raise the threat, to varying degrees, of the Internet's accelerating fragmentation.

Rather than seeing the Internet's fragmentation as the prelude to a complete "decoupling" of networks, this study conceives of it as a slow process of "re-connectivity", reshaping the Internet's configuration so as to exert an influence on the data flows circulating between different actors. Sino-American competition underpins – and dominates – this paradigm, which encompasses four dimensions: geopolitical, technological, legal and commercial. In this context, the discourse surrounding fragmentation is ambiguous. It covers a multitude of complex and complementary phenomena, as well as serves to maintain the *status quo* in favor of U.S. foreign policy and economic interests in global Internet governance forums. This study, however, looks beyond the United States, comparing the initiatives of other national players – China, Russia, India and the European Union. These actors' policies could be described as pursuing fragmentary strategies, although their distinct political regimes prevent us from comparing them directly to one another.

3. See J. Nocetti (ed.), "Souveraineté numérique : dix ans de débats, et après ?", *Annales des Mines – Enjeux Numériques*, No. 23, September 2023.

Semantics and challenges of recurrent Internet fragmentation

The potential for partition

The notion of Internet "fragmentation" is regularly discussed via the vocabulary of partition. The splintering of the network of networks, or even the secession of certain parts of the Internet, is often referred to as "balkanization". The term, used since the 1940s in constitutional and commercial debates in the United States, refers to the process of partitioning a state into smaller, independent entities, and unsurprisingly has negative connotations. The term was first used in connection with the Internet in 1997, in an MIT study. Marshall van Alstyne and Erik Brynjolfsson argued that the growth of a global communications infrastructure would not necessarily lead to the emergence of a "global Internet village" – it could also fragment societies and "balkanize" interactions in the emerging digital space.[4]

The term "balkanization" was given new currency during the first World Summit on the Information Society (WSIS), held in Tunis in 2005 and sponsored by the United Nations. The summit was the culmination of almost four years of negotiations on the participation of various stakeholders (governments, civil society, private actors) in the development of rules for the Internet. It witnessed the emergence of what was to become a fundamental opposition between authoritarian regimes and the proponents of a multi-stakeholder model guaranteeing the values of openness and interoperability espoused by the founders of the Internet. Intellectuals such as the American legal scholar Tim Wu – who stresses how censorship and regulatory constraints can drive the balkanization of the Internet[5] – or the Japanese entrepreneur Joichi Ito, who has warned of possible consequences of the internationalization of domain name system (DNS) management on a unified Internet[6], have voiced some early concerns.

4. M. van Alstyne and E. Brynjolfsson, "Electronic Communities: Global Village or Cyberbalkans?", Massachusetts Institute of Technology, March 1997, available at: https://web.mit.edu/.
5. J. Goldsmith and T. Wu, *Who Controls the Internet? Illusions of a Borderless World*, New York: Oxford University Press, 2006. See also T. Wu, "The Filtered Future", *Slate*, July 11, 2005, available at: https://slate.com/. Tim Wu suggests that Internet users don't regularly visit other countries' websites, that sites like Google become national (abroad) through the use of geolocation software, and that local traffic is growing much faster in (mainland) China than traffic routed over its international channels.
6. J. Ito, "The Internets", Joichi Ito' blog, July 11, 2005, available at: https://joi.ito.com/.

Alongside "balkanization", the notion of a "Splinternet" has also been introduced. A portmanteau of "splinter" and "Internet", it describes a section of the Internet that, for technological, commercial or political reasons, might break away and become inaccessible to other parts of the network. First used in 2001 by libertarian expert Clyde Wayne Crews, the term was intended to describe an ideal – the creation of parallel, privately managed and autonomous Internets which could unleash the infinite potential of the Internet[7] – rather than a phenomenon arising in defiance of the technical and political fundamentals of the global network. This view, which resonates with the Internet's earliest communities, is grounded in the defense of the individual as a consumer: rather than navigating within a restrictive cyberspace, atrophied by governments' attempts to regulate it (fighting spam, limiting access to certain types of content, etc.), consumers should organize themselves in proprietary, corporate networks, giving them access to personalized content and services.[8]

The concept gained new momentum in 2010. John Bernoff, president of Forrester Research, sees the proliferation of non-interoperable devices, operating systems and applications as evidence of the failure of the open, collaborative Internet utopia.[9] The Internet, which was supposed to "flatten" the world, has instead become the foundation for a new paradigm in which the proprietary principles of certain dominant or even oligopolistic actors – Apple, Google, Amazon, etc. – make it harder for users to get out. This reasoning is echoed in the description of how ISPs undermine the principle of net neutrality, which advocates for equal treatment of all data in circulation – regardless of content, platform or recipient – without any restrictions applied by the actors of the digital economy.[10] The concept of "enclosure" serves to describe the strategies employed by major digital platforms to leverage the data of captive users.[11]

More broadly, the description of the global network's segmentation illustrates its constantly shifting course, caught between the struggle to maintain its universality and a trend towards regionalization.[12] For some, this dichotomy echoes the old debate between a utopian vision of the democratization of society and the liberation of information through the Internet, and the clash of the "information revolution" with state-imposed regulations.[13]

7. C.W. Crews, "One Internet Is Not Enough", CATO Institute, April 11, 2001, available at: www.cato.org.
8. *Ibid.* See also M. Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge, MA: MIT Press, 2010.
9. J. Bernoff and S. van Boskirk, "The Splinternet", Forrester, January 26, 2010, available at: 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", Ministry of Foreign Affairs, August 2020, available at: www.diplomatie.gouv.fr.
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.

Finally, and in connection with fragmentation, the concept of "alignment" refers, according to Milton Mueller, to deliberate or unintentional processes which result in the Internet's gradual centralization at the national level, through a variety of means: Internet securitization, in accordance with governmental ambitions; the territorialization of data flows; and initiatives designed to structure the control of critical Internet resources within a national framework.[14] Proponents of this approach would stand in opposition to a self-regulating Internet, a so-called multistakeholder system founded on participatory mechanisms for the governance of Internet infrastructure and usage.[15] One extreme example of the Internet's "alignment" with state jurisdictions came when Edward Snowden exposed the extent of U.S. digital espionage, sparking widespread political debate around the world.[16] And since the 2015-2016 attacks targeting France and its European neighbors, the readjustment of national laws with respect to Internet control mechanisms has again raised the issue of alignment. The growing use of digital surveillance technologies within democracies (deployment of automated border control systems, predictive policing and facial recognition systems), demonstrates an increasing reliance on tried-and-tested technologies.

Three types of fragmentation

The fragmentation of the Internet can take many forms, and assessing the threat this represents for the global network will vary according to whether we conceptualize the Internet as a purely technical infrastructure or as a globalized public sphere.[17] The abundance of commentary detailing the Internet's fragmentation has not, however, resulted in a consensus on the nature of this process of division or on the urgency with which it should be remedied.

Technical fragmentation

Technical fragmentation is the perspective through which the risks of global network breakdown are most often analyzed. Some apply an extensive interpretation: Milton Mueller defines this type of fragmentation as:

> "an *intentional* defection from the global Internet, led by a group of actors capable of taking with them a *substantial segment of the world's population*; this defection must

14. M. Mueller, *Will the Internet Fragment?*, Cambridge: Polity, 2017.
15. B. de La Chapelle, "Gouvernance Internet : tensions actuelles et futurs possible", *Politique étrangère*, Vol. 76, No. 2, p. 252-253, available at: www.cairn.info. For a critical perspective about multistakeholderism, see F. Massit-Folléa, "Internet et les errances du *multistakeholderism*", *Politique étrangère*, Vol. 79, No. 4, Ifri, 2014, pp. 29-41.
16. J. Nocetti, "Puissances émergentes et internet : vers une troisième voie ?", *Politique étrangère*, Vol. 78, No. 4, 2014, p. 43-55.
17. C. Perarnaud, J. Rossi, F. Musiani and L. Castex, "'Splinternets': Addressing the Renewed Debate on Internet Fragmentation", *Study*, European Parliament Research Service, Panel for the Future of Science and Technology, 2022, p. 11.

> succeed in establishing effective *technical incompatibilities* between their part of the Internet and the other part(s); and these incompatibilities must be both *sustainable* over a significant period of time and able to *obstruct communications among parties that are willing to communicate*."[18]

For others, the technical aspects of Internet fragmentation should focus on the risks to network interoperability and technical barriers to data transfer.[19] In essence, it therefore results from decisions which, deliberately or not, permanently or temporarily, break or limit digital connectivity between one part of the Internet and the rest of the network.[20]

Samuele Dominioni groups the processes of technical fragmentation in terms of the security risks that can affect the Internet's core resources, namely:

- naming (management of the Domain Name System (DNS), the technical foundation of the Internet);
- addressing (assignment of communication protocol and physical IP network numbers);
- data routing.[21]

Addressing-related issues were identified as early as the 2000s: in *Protocol Politics*, Laura DeNardis described how the gradual scarcity of IPv4 addresses had prompted states to invest in IPv6, a more recent technology that was not then dominated by American interests and companies.[22] Yet the still sporadic adoption of IPv6[23] accentuates the fragmentation process, due to the technical incompatibility between IPv4 and IPv6.[24] ISPs' lack of responsiveness in the transition to IPv6 has been criticized, particularly in the United States, where they have sought to avoid the costs associated with an interoperability upgrade[25]. Lastly, the process of configuring terminals via IPv6 is likely to increase digital vulnerabilities and, more generally, the attack surface.[26]

Another issue related to addressing is the hypothesis that uncoordinated national Internet Protocols, or those in direct conflict with the existing system, could significantly disrupt the accessibility and security of national

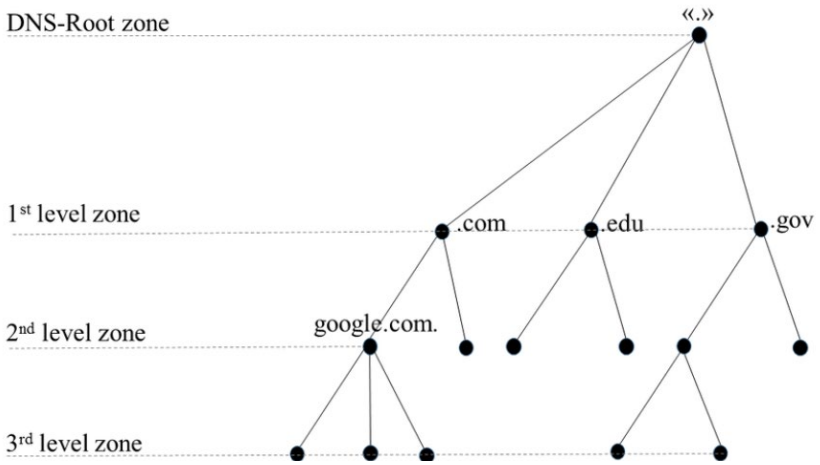
18. M. Mueller, *Will the Internet Fragment?*, *op. cit.*, p. 43. Italics in the original.
19. W. Drake, V. Cerf and W. Kleinwächter, "Internet Fragmentation: An Overview", *White Paper*, World Economic Forum, January 2016, p. 4, disponible sur : www.weforum.org.
20. C. Perarnaud, *et. al.*, "'Splinternets' [...]", *op. cit.*, p. 4.
21. S. Dominioni, "Internet Fragmentation and Cybersecurity: A Primer", UNIDIR, 2023, available at: https://unidir.org/.
22. L. DeNardis, *Protocol Politics: The Globalization of Internet Governance*, Cambridge, MA: MIT Press, 2009, p. 97-138.
23. Mapped and updated by Google, the adoption of IPv6 varies widely: in January 2024, only five countries broke 60% (France, Germany, India, Malaysia and Saudi Arabia). See www.google.com.
24. E. Bais, "IPv4 vs IPv6: What Security Professionals Should Know", Prefix Broker (undated), available at: www.prefixbroker.com.
25. 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, 2012, p. 22-24, available at: www.belfercenter.org.
26. See for example "Transition vers IPv6", press release by ARCEP and Internet Society France, December 18, 2019, available at: www.arcep.fr.

networks. This would mean governments would have to enter into bilateral agreements with access providers and ensure the security of their own network protocols and standards.[27]

Naming concerns essentially point to threats to the Domain Name System (DNS), a hierarchical system enabling IP addresses to be expressed as intelligible words in place of a string of numbers. The DNS root zone is the top-level DNS zone in the Internet domain name system. It refers to name servers for Top-Level Domains (TLDs: .com, .org, as well as country codes such as .fr, .jp, etc. See diagram on next page). Domain names are translatable into one or more IP addresses, and these addresses can be modified without changing the domain name. This means that if a website chooses to relocate a server to a new IP address, it does not need to change its domain name. The DNS root zone is controlled by thirteen "identities" or clusters of DNS root servers, which act as the authority for requests to top-level domains. Twelve organizations control these servers: nine American, two European and one Japanese. For nine of these servers, the technical architecture is also distributed in different geographical locations: as of January 2024, 1,756 sites in 59 countries host a DNS root server.[28]

From 1998 to 2016, a Californian company (the Internet Corporation for Assigned Names and Numbers – ICANN) managed the DNS root, the allocation of IP addresses and the maintenance of the system's protocols with the Internet Engineering Task Force (IETF), through a contractual agreement with the US Department of Commerce. This made the issue of technical supervision a central theme of many debates in international forums tasked with defining the contours of global Internet "governance".[29]

Figure 1: DNS logical architecture1



Source: R. G. Alakberov et. al., "Internationalized top level domain names: their registration and problems", Problems of information society, 2017, No. 1, p.45

27. S. Dominioni, "Internet Fragmentation and Cybersecurity: A Primer", *op. cit.*, p. 11.
28. Data compiled on https://root-servers.org/.
29. See J. Nocetti (ed.), "Internet, une gouvernance inachevée", *Politique étrangère*, Vol. 78, No. 4, 2014, pp. 10-81.

The vast and complex issue of the DNS has prompted many fears concerning its fragmentation, both through the development of "national segments" and the demands of certain states for the de-Americanization of the systems used to manage the Internet's critical resources.[30] In 2010, for example, a coalition led by Russia, together with China, submitted a proposal to the International Telecommunications Union (ITU) to give states veto power over decisions adopted by the ICANN Board on naming and addressing issues. Moscow and Beijing coordinated their efforts to secure the introduction of national top-level domain names in non-Latin scripts that same year, in a parallel effort to promote a multilingual Internet.[31] It is also worth noting that attempts to rival ICANN over the root of the Internet have attracted limited interest: the RINA (Recursive InterNetwork Architecture) protocol, developed in 2008 by John Day as an alternative to the original TCP/IP, has only been partially adopted by Armenia and the Vatican.[32]

Last but not least, the Internet's topology is maintained by the Border Gateway Protocol (BGP), which ensures the global network's routing operations, connecting the many subnetworks that make up the Internet, and enabling the routing of data from point A to point B. These broad highways of the Internet also arouse states' ambitions and can lead to a dynamic of fragmentation. For Russia and Iran, for example, control over the routes through which data is transmitted affords them a number of advantages that their authorities will seek to exploit: filtering, spying on or diverting data flows.[33] The sophistication and lack of transparency of the BGP architecture means that it can easily be manipulated for strategic purposes. This is also true from a competitive standpoint, which has implications in terms of fragmentation: "the concentration of data flows in the hands of a few major routing specialists and large platforms such as Google, Facebook and Amazon" raises questions concerning the free circulation of data, its integrity and sovereignty, all the more so when outages are becoming more frequent for some of their services.[34] Finally, the democratization of virtual private networks (VPNs) is sometimes likened to a form of fragmentation, as users become isolated from the global Internet; conversely, some states restrict or prohibit the use of VPN

30. See F. Musiani, D. Cogburn, L. DeNardis and N. Levinson (ed.), *The Turn to Infrastructure in Internet Governance*, New York: Palgrave Mcmillan, 2016.
31. A. Bhuiyan, *Internet Governance and the Global South. Demand For a New Framework*, Basingstoke: Palgrave Mcmillan, 2014, pp. 97-112.
32. J.-A. Fines, "RINA, un projet pour l'internet de nouvelle génération", *La Revue européenne des médias et du numérique*, September 24, 2019, available at: https://la-rem.eu/.
33. Concerning Russia, see K. Limonier, "Vers un 'Runet souverain' ? Perspectives et limites de la stratégie russe de contrôle de l'Internet", *Echo*Géo (online), No. 56, 2021, available at: https://journals.openedition.org/. On Iran's strategy, see L. Salamatian, F. Douzet, K. Salamatian and K. Limonier, "The Geopolitics Behind the Routes Data Travel: A Case Study of Iran", *Journal of Cybersecurity* (online), Vol. 7, No. 1, 2021, available at: https://academic.oup.com/.
34. F. Douzet, "La panne de Facebook révèle l'urgence de penser des solutions pour favoriser la décentralisation d'Internet", *Le Monde*, October 11, 2021, available at: www.lemonde.fr.

protocols to prevent their citizens from anonymizing their Internet traffic.[35]

(Geo)political fragmentation

The (geo)political dimension of fragmentation is fuelled by the Internet's growing territorialization. For Milton Mueller, the fragmentation of the Internet is a product of rhetorical obfuscation, and actually represents states' efforts to "align" the Internet with their national borders. A power struggle over the future of the very notion of sovereignty in a digitized world, the debate over fragmentation transcends the scope of the Internet and its technical oversight to include dynamics which are fundamentally geopolitical in nature.[36]

In this sense, control over data has become the issue through which this political fragmentation is most tangible. The principle of the free flow of data – the cornerstone of the convergence of economic globalization and the rise of digital technology – has been and continues to be challenged on many levels and in a variety of different forms, by authoritarian regimes and democratic states alike. The revelations made by Edward Snowden in June 2013 were a major turning point, illustrating this growing threat to freedom from national frameworks. The politicization of personal data localization practices has since become an issue of national sovereignty and global competition.[37]

For states, this territorialization of the Internet is legitimized through law. The differences in their approaches are largely a reflection of the nature of their respective political regimes. While some – mainly authoritarian – states prefer to physically locate personal data within their borders, other states, such as Brazil, have preferred to legally bind companies collecting, storing or processing the personal data of their citizens through Brazilian privacy laws.[38]

Alongside legal instruments, state policies to retain control over data produced by their citizens have also included supporting the development of national actors, especially in the cloud, limiting foreign investment in the data center industry, and even duplicating citizens' data within national borders.[39] Critics of such measures denounce them as contributing to the Internet's fragmentation, whether they are protectionist (to adjust the rules

35. W. Drake, V. Cerf and W. Kleinwächter, *op. cit.*, p. 24.
36. M. Mueller, *Will the Internet Fragment?*, *op. cit.*, p. 3.
37. T. Gomart, J. Nocetti and C. Tonon, "L'Europe, sujet ou objet de la géopolitique des données ?", *Études de l'Ifri*, July 2018, available at: www.ifri.org.
38. M. Maciel and B. Martins dos Santos, "Brazil: A 'Soft' Digital Power", in A. Pannier (ed.), "The Technology Policies of Digital Middle Powers", *Études de l'Ifri*, Ifri, February 2023, pp. 24-25, available at: www.ifri.org. See also A. Cattaruzza, "Quelle souveraineté pour l'espace numérique ?", *in* S. Taillat, A. Cattaruzza and D. Danet (ed.), *La Cyberdéfense. Politique de l'espace numérique*, Paris: Armand Colin, 2018, pp. 88-89.
39. T. Gomart, J. Nocetti and C. Tonon, "L'Europe, sujet ou objet de la géopolitique des données ?", *op. cit.*, p. 19.

of the competitive asymmetry with the major U.S. tech firms), security-oriented (to defend against foreign surveillance) or geopolitical (to denounce aggressive U.S. activities in cyberspace).[40]

While data localization practices are not necessarily intended to "fragment" the Internet, voluntary interruptions of access to the global network (Internet shutdowns) do imply a deliberate act. Voluntary Internet outages are a growing phenomenon, affecting 35 countries in 2022 (187 incidents that year, compared with 159 in 2020). According to the NGO Access Now, between January and May 2023, 21 states took the initiative to cut off Internet access (80 cuts in total): while these are mainly authoritarian regimes (China, Russia, Iran, etc.), the country responsible for the greatest number of suspensions is India, for a range of reasons (preventing violent backlash in provinces embroiled in separatist struggles, such as Kashmir, but also to prevent cheating during exams).[41] Some regions plagued by conflict or civil war, such as Myanmar or Tigray in Ethiopia, are also regularly disconnected from the global Internet by their authorities.[42] While these practices are mainly observed during periods of acute political tension and crisis, such as in Iran in 2019 and from September 2022 onwards,[43] intentional shutdowns have very real consequences for affected populations, in terms of access to employment, income or even food. In India, for example, mobile Internet access is often a prerequisite in order to use applications that provide access to social security, employment rights and food rations.[44] While kill switches may appear to be the ultimate expression of sovereign power, they also reveal decision-makers inability to extend state sovereignty to the digital realm.[45]

Lastly, the process of "territorializing" the Internet also has a strategic dimension. Whether by taking control of a network's physical infrastructure (as in Ukraine[46]), or destroying a country's Internet infrastructure and mobile connectivity (as in Gaza beginning in October 2023[47]), military conflicts are a concrete demonstration of how the development of offensive

40. W. Drake, V. Cerf and W. Kleinwächter, *op. cit.*, p. 41-45; J. Force Hill, *op. cit.*, pp. 46-47.
41. See "An Overview of Global Internet Shutdowns", Access Now, May 19, 2023, available at: www.accessnow.org; "Who Is Shutting Down the Internet in 2023? A Mid Year Update", Access Now, July 31, 2023, available at: www.accessnow.org.
42. "Internet Shutdowns Have Become a Weapon of Repressive Regimes", *The Economist*, October 15, 2021, available at: www.economist.com.
43. M. Burgess, "Iran's Internet Shutdown Hides a Deadly Crackdown", *Wired*, September 23, 2022, available at: www.wired.com.
44. "'No Internet Means No Work, No Pay, No Food' Internet Shutdowns Deny Access to Basic Rights in 'Digital India'", report by NGOs Human Rights Watch and the Internet Freedom Foundation, 2023, available at: www.hrw.org.
45. M. Mueller, *op. cit.*, p. 91.
46. For an account of Russia's manipulation of the BGP protocol in Ukraine since 2014, see 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, pp. 157-182.
47. M. Burgess, "The Destruction of Gaza's Internet Is Complete", *Wired*, October 27, 2023, available at: www.wired.com.

capabilities can have an impact on the international stage. This aspect of fragmentation, though little studied as of yet, carries very real risks for the stability and resilience of cyberspace.

Commercial fragmentation

Beyond the geopolitical justifications for fragmentation, the economic stakes at play are not to be underestimated, whether they concern protectionist strategies adopted by national authorities (e.g. in China or the United States) or strictly commercial strategies. Given the business model of the major digital platforms – advertising revenues tied to user data files – this commercial dynamic drives companies like Meta and Google to develop their proprietary technology platforms in order to retain their users and monetize the content they produce and exchange.

These technological ecosystems have become opaque "walled gardens", creating a situation of complete dependence for users. Control over this data is a strategic source of revenue, prompting these companies to restrict data exchanges, or even make all forms of reciprocal research and data exchange incompatible. For example, Google and Meta (Facebook, Instagram, WhatsApp) have been mutually blocking all data transfers between their different applications since 2010.

This commercial fragmentation also reflects the process of the Internet's "platformization", the digital economy's most consolidated actors being driven to build and own their own technical infrastructure. By deploying their own submarine cables, installing their own in-house protocols based on proprietary technologies, and gaining direct access to the data of billions of captive consumers, Google, Meta and Amazon are in a way creating their own networks, while at the same time becoming the main gateway to the global Internet.[48] As catalysts of data and infrastructure fragmentation, Web companies and telecom firms are also closely involved in issues of network neutrality and intellectual property protection.[49]

Is the issue of fragmentation primarily a U.S. concern?

The three dimensions of Internet fragmentation, beyond the sovereign dynamics that permeate the global network, cannot be dissociated from the evolution of U.S. foreign and security policies. The Internet has long been portrayed by American diplomacy as a global infrastructure in order to defend its own interests. The instrumentalization of its – privatized –

48. C. Perarnaud quoted in L. Gamaury, "Splinternet: Quand la menace d'une fragmentation d'Internet se précise", *20 Minutes*, October 4, 2022, available at: www.20minutes.fr.
49. W. Drake, V. Cerf and W. Kleinwächter, "Internet Fragmentation: An Overview", *op. cit.*, pp.50-52 and 56.

backbone now represents one of the key factors of the Internet's "fragmentation" in specialized international forums.

From an American perspective, this process was historically driven in three phases. Firstly, in the early days of the post-Cold War era, the United States, amid a process of deregulation designed to provide market opportunities for its businesses, promoted the narrative of a nascent, horizontal Web, with no cost of entry, accessible without needing to rely on any one company. The Internet's critical resources were likewise considered borderless: the U.S. government dismissed laws applicable to servers as incongruities. This approach was echoed in Vice President Al Gore's (1993-2001) speech at the 1994 ITU conference in Buenos Aires[50]. The popularity of John Perry Barlow's 1996 "Declaration of the Independence of Cyberspace", with its libertarian overtones, prompted U.S. diplomats to reprise the narrative of the Internet as a global project: not a collectively developed U.S. infrastructure, but a "global information infrastructure"[51].

The second phase was defined by two intertwined processes converging to exploit the Internet's infrastructure for national security purposes after September 11, 2001. On the one hand, U.S. authorities allowed the digital platform and service provider market to consolidate around a handful of national firms. On the other hand, Washington began to reinterpret the Internet as a tool of strategic coercion; an instrument through which data could either be secretly extracted from targets (*via* espionage programs[52]); or disseminated to targets within states seeking to limit digital traffic (by means of public diplomacy reconfigured around digital tools[53]). These overlapping strategies of market consolidation and the heightened surveillance of the war on terror served to streamline relations between the American intelligence apparatus and private Internet companies.

The third phase began with the 2016 U.S. presidential campaign, when the West came to recognize U.S. adversaries' intensifying Internet activities (cyber-attacks, informational manipulation, etc.). For Washington, this entailed blocking or cutting off access to the Internet's critical infrastructure for players hostile to the United States. While missions developed since 2001 are still ongoing – and have made data the primary focus of Washington's economic redeployment and security strategy – the United States now threatens certain states with exclusion from critical sectors of the Internet.

50. "Inauguration of the First World Telecommunication Development Conference", speech by Vice President Al Gore, Buenos Aires, March 21, 1994, available at: https://search.itu.int/.
51. "The Global Information Infrastructure", *White Paper*, White House Forum on the Role of Science and Technology in Promoting National Security and Global Stability, March 29-30, 1995, available at: https://clintonwhitehouse4.archives.gov/. See also "Global Information Infrastructure and Global Information Society", *OECD Digital Economy Papers*, No. 18, OECD, 1996, available at: www.oecd-ilibrary.org.
52. See E. Snowden, *Permanent Record*, New York: Metropolitan Books, 2019.
53. J. Nocetti, "La diplomatie d'Obama à l'épreuve du Web 2.0", *Politique étrangère*, Vol. 75, No. 1, pp. 157-169.

The shift of the Internet's demographic center of gravity towards Asia, and the U.S.'s relative failure to achieve its goals in Internet governance forums, explain Washington's interest in accelerating a process of fragmentation, to ensure that the U.S. can dictate the terms of network connectivity processes. In 2020, during Donald Trump's presidency, the Clean Network Program was designed to purge U.S. networks (and its partners) of "untrusted" Chinese applications and equipment (TikTok, WeChat, Huawei, etc.) The "Clean Network" was to give the U.S. the means to dictate entry conditions by requiring its partners to exclude Chinese companies from all layers of the Internet, including connectivity infrastructure. This initiative contributed to the fragmentation of the Internet, which Washington has traditionally criticized. While the Biden administration has not reclaimed this "Clean Network" label, it continues to actively campaign against Chinese suppliers, in particular Huawei, when engaging with its partners[54]. More broadly, it has made friendshoring – establishing the political dependability of partners as an essential factor in the structuring of global supply chains – a central feature of the reorientation of its Internet diplomacy, aiming at "decoupling" from China.

Beyond international debates which sometimes promote fragmentation as part of a demand for change in Internet governance processes, the impact of the U.S. on the dynamics of fragmentation cannot be overlooked. It is, in fact, a structural factor driving the discourse on China. Washington's announcement, for example, that it is withdrawing its 2019 proposals to the World Trade Organization (WTO) – to prohibit states from imposing measures on the storage or processing of data on their soil and the examination of software source code – has reinforced the perception of the U.S. as pursuing a policy of containment of China's digital strategy.[55]

54. See M. Velliet, "Convince and Coerce: U.S. Interference in Technology Exchanges Between Its Allies and China", *Études de l'Ifri*, Ifri, February 2022, available at: www.ifri.org; J. Sakellariadis and L. Pfahler, "Transatlantic Blame Game: Trump, Merkel, Biden and the Danger of Germany's Dependence on Huawei", *Politico*, October 15, 2023.
55. D.Lawder, "U.S. Drops Digital Trade Demands at WTO to Allow Room for Stronger Tech Regulation", Reuters, October 26, 2023, available at: www.reuters.com.

An alternate perspective on Internet fragmentation: initiatives from four actors

The scenario of Internet fragmentation is often presented as an opposition between the West and "the rest" – that is, in most analyses, an alternative under Chinese control.[56] Such a binary reading is outdated in 2024, so profoundly has this field transformed since the intensification of Sino-American technological competition and the outbreak of Russia's invasion of Ukraine. The United States, China and the European Union each have a distinct vision of digital capitalism. These visions lead to forms of "fragmentation", to varying degrees, which should be considered hierarchically. Including Russia and India in this reading is crucial to understanding the political dynamics underlying these centrifugal trends.

China: a global strategy of fragmentation

Digital and technological factors play a key role in China's international ambitions. China is pursuing a long-term effort to gain technological ground and disrupt the United States' domination of the digital space.

The country also contributes significantly to the fragmentation of the global Internet for domestic political purposes: the "Great Firewall" has, since the early 2000s, exemplified China's staunch control of the Internet at the national level through censorship which has been integrated into the very architecture of the Chinese network, where the services of major American companies such as Facebook, Twitter and YouTube have been banned since 2009, and Google since 2010.

Setting future technical standards

China recognizes the strategic impact of developing and imposing technical norms and standards for the Internet, and has helped establish it as a key issue in international relations.[57] In 2018, Huawei announced its plan for a "decentralized Internet infrastructure" at the ITU, claiming that the current Internet was facing "fundamental problems" and critical vulnerabilities connected with increasing cyber-attacks, its centralized architecture and the

56. A. Barrinha and T. Renard, "Power and Diplomacy in the Post-Liberal Cyberspace", *International Affairs*, Vol. 96, No. 3, 2020, p. 765, available at: https://academic.oup.com/.
57. J. Seaman, "China and the New Geopolitics of Technical Standardization", *Notes de l'Ifri*, Ifri, January 2020, available at: www.ifri.org.

multiplication of biases.[58] In September 2019 – at the height of Sino-American tensions – Chinese delegations reiterated their call for a "decentralized Internet", to be known as "New IP", at meetings of the ITU's telecommunications standardization sector and during Internet Engineering Task Force (IETF) meetings.[59] This technology purports to overhaul the Internet's original technical architecture and TCP/IP protocol to support the growth of emerging applications (telemedicine, autonomous cars, holographic communications, etc.). It also incorporates a stop protocol enabling a central entity to isolate an IP address from the rest of the network. Addresses, as well as packets sent and received, would be connected to the identity of the computer owner or connection holder. The initiative has met with strong reactions from the Internet's multistakeholder communities, who are generally in favor of maintaining the *status quo* in terms of Internet governance. It does, however, illustrate Beijing's aim to use technology to promote a different form of Internet governance, in addition to an alternative Internet.[60] Between 2020 and 2022, a number of debates concerning interoperability delayed New IP's progress at the ITU. But by 2021, China's positions on the project were being disseminated in proposals to the UN body.[61]

There are two possible readings of the "New IP" proposal. On the one hand, rather than decentralizing the Internet, this project, which reconfigures founding Internet principles such as trust mechanisms (e.g. public infrastructures, use of encryption, etc.), domain names and Internet protocols, serves to legitimize the broader framework of Chinese foreign policy and, with respect to the Internet, the state-centered governance model that drives it.[62] This interpretation is inextricably linked to broader fears surrounding China's efforts to export its model of digital authoritarianism.[63] On the other hand, some argue that the economic motives behind the "New IP" initiative should not be underestimated, focusing instead on the control and surveillance capabilities Beijing is deploying across digital networks.[64]

Where standardization is concerned, Huawei holds a similarly central role in the proposal for the IPv6+ protocol, presented as an enhanced version of IPv6. First conceived in 2019, the Chinese initiative only appears in ITU

58. See "Decentralized Internet Architecture", Light Reading, November 20, 2018, available at: www.lightreading.com.
59. The document presented by Huawei at the event, "New IP: Shaping the Future Network", is available at: www.itu.int.
60. M. Murgia and A. Gross, "Inside China's Controversial Mission to Reinvent the Internet", *Financial Times*, March 27, 2020, available at: www.ft.com.
61. See "Global Connectivity Report 2022", International Telecommunication Union, 2022, available at: www.itu.int.
62. S. Hoffmann, D. Lazanski and E. Taylor, "Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet", *Journal of Cyber Policy*, Vol. 5, No. 2, 2020, p. 255, available at: www.tandfonline.com.
63. N. Inkster, *The Great Decoupling: China, America and the Struggle for Technological Supremacy*, London: Hurst, 2020, pp. 157-158.
64. A. Mueller and C.S. Yoo, "Crouching Tiger, Hidden Agenda? The Emergence of China in the Global Internet Standard-Setting Arena", *Research Paper*, No. 23-33, University of Pennsylvania, Institute for Law and Economics, August 2023, available at: https://papers.ssrn.com/.

documents starting in 2022, where it is presented as a natural extension of IPv6 rather than a radically new architecture.[65] As with "New IP", this project cannot be divorced from commercial considerations, the business product taking precedence over the technical protocol designed to support the rapid growth in the number of connected terminals. Sub-Saharan Africa is thus an object of keen interest in this area, within the broader context of the New Digital Silk Roads.[66] The uncertainties surrounding this protocol's functionalities, and in particular the potential additional data requirements it may impose on all Internet traffic, add to the perception of a risk of fragmentation.[67]

Hardware: unbridled exports at the intersection of geopolitics and trade

China is increasing its efforts to become self-sufficient in digital equipment, and to export its own hardware. Its strategy is built upon overt protectionism and conspicuous state support for mobile Internet infrastructure (5G base stations), satellite navigation (Beidou), undersea cables and, increasingly, satellite Internet.

Beijing's efforts to secure its supply chains – together with Western responses, which political authorities regard as an additional risk factor – may drive commercial and legal fragmentation of hardware applications, eventually resulting in very real technological fragmentation, with different technical hardware standards coexisting on a global scale.[68] Revisions to the cybersecurity legislative framework (in 2013 and 2017) have considerably restricted foreign equipment manufacturers' freedom of action in China.[69]

Chinese equipment manufacturers' success on the export market contributes to the spread of commercial and legal fragmentation globally. Chinese projects are most often undertaken as part of bilateral agreements, making contractors technologically and financially dependent over the long term, a situation that could fuel expectations of "decoupling".[70] The U.S. Clean Network program's criteria and tone palpably mirror this situation.[71]

65. L. Bertuzzi, "La Chine modifie sa proposition sur la gouvernance d'Internet et cible les pays en développement", Euractiv, June 7, 2022, available at: www.euractiv.fr.
66. H. Tugendhat and J. Voo, "China's Digital Silk Road in Africa and the Future of Internet Governance", *Working Paper*, No. 50, China-Africa Research Initiative, School of Advanced International Studies (SAIS), Johns Hopkins University, 2021, available at: www.econstor.eu.
67. L. Bertuzzi, "La Chine modifie sa proposition sur la gouvernance d'Internet et cible les pays en développement", *op. cit.*
68. K. von Carnap, A. Hmaidi, R. Arcesati and J. Groenewegen-Lau, "Fragmenting Cyberspace: The Future of the Internet in China", *MERICS Report*, MERICS, November 2023, p. 48, available at: https://blog.merics.org/.
69. See N. Alsabah, "China's Cyber Regulations: A Headache for Foreign Companies", *Comment*, MERICS, March 22, 2017, available at: https://merics.org/.
70. N. Inkster, *The Great Decoupling: China, America and the Struggle for Technological Supremacy*, *op. cit.*
71. See M. Rithmire and C. Han, "The Clean Network and the Future of Global Technology Competition", *HBS Case 721-045*, Harvard Business School, April 12, 2021, available at: https://globaltechsecurity.com/.

Beijing sees the Internet's infrastructure as a strategic entity in which national actors must be involved. Huawei – though to a lesser extent since U.S. sanctions – or HMN, a vertically-integrated cable company (as well as an operator), receive significant state support, enabling them to strengthen their market share. HMN (Huawei Marine Networks, a subsidiary of the Hengtong Group) deployed the *Pakistan & East Africa Connecting Europe* (PEACE) cable – a component of the New Silk Roads connecting the Pakistani and French coasts via Kenya – and, in Europe, laid the *Silphium* cable between Greece and Libya, as well as the *Hannibal* cable between Sicily and Algeria.[72] Since 2022, however, U.S. pressure on cable projects involving one or more Chinese stakeholders (even without the participation of U.S. companies) has resulted in projects either being frozen or Chinese cable companies being excluded. This was the case for the aborted *Cap-1* cable project, which would have run from California to Singapore *via* Hong Kong and Malaysia; the *Sea-Me-We 6* project between Singapore and Marseille, awarded to U.S. company SubCom over HMN; and the *Medusa* (connecting Egypt to Portugal) and *Africa-1* (running from Kenya to France) cables, awarded to France's ASN rather than HMN, which had been invited to bid.[73] The activism of Chinese players in submarine cable-laying - an industry that has become highly competitive – illustrates a broader trend. Through technological assistance policies, China, like the United States, is reconfiguring global digital networks, and consequently the conditions of interdependence, to its advantage. On the African continent, infrastructure-related issues play a key role in the competition between Chinese and Western players.[74]

Applications: WeChat and the strategy of layered fragmentation

Along with TikTok, WeChat stands as the most notable success story of China's digital economy and of its exportation beyond the country's borders. The technical characteristics of this "super-application" (containing a series of mini-programs, each with their own application environment) limit interconnectivity between the different parts of the network, leading to technical fragmentation. Today, the platform is more akin to a new type of infrastructure, with a collection of "walled gardens" built one inside the

72. J. Brock, "U.S. and China Wage War Beneath the Waves – Over Internet Cables", Reuters, *Special Report*, March 24, 2023, available at: www.reuters.com. See also D. Aluf, "China's Subsea-Cable Power Play in the Middle East and North Africa", *Issue Brief*, Atlantic Council, May 2023, available at: www.atlanticcouncil.org.
73. A. Gross, A. Heal, C. Campbell, *et. al.*, "How the U.S. Is Pushing China Out of the Internet's Plumbing", *Financial Times*, June 13, 2023, available at: https://ig.ft.com/subsea-cables/.
74. J. Carver, "Developing Digital Peripheries for Strategic Advantage: A Comparative Analysis of American, EU, and Chinese Projects in Africa", paper presented at The Hague Conference on International Cybersecurity, Leiden University, November 6, 2023.

other, like nesting dolls.[75] Indeed, programmers developing applications for the mini-program infrastructure must use WeChat's proprietary scripting language, accessible only via the application's interface. Compared with companies like Apple, which are also committed to creating "walled gardens", WeChat features multiple layers of fragmentation: compatibility between smartphones for the application's mini-programs; a restrictive registration process; geo-locked features.[76]

These three examples are by no means exhaustive, as the fragmentation resulting from China's digital policies has become so varied. One underlying trend is that Chinese authorities are seeking to extend their data governance laws (data collection, processing and transfer, as well as trade) extraterritorially, for both political (challenging the perceived hegemony of U.S. law, defending a specific approach to data sovereignty) and economic purposes (supporting the deployment of the Digital Silk Road).[77] This combination of political and economic motives is part of a Chinese strategy that blends security interests with the exploitation of the openness specific to the Silicon Valley ecosystem.[78]

Russia: towards a split from the global Internet

The Russian authorities' political approach to the Internet closely links domestic and external factors. Public statements by decision-makers and legislative activity tie in with regional and international political initiatives, while global events in turn influence Russia's digital strategy[79]. The keyword in Russian digital policy is sovereignty, which must be considered from a strategic, informational and economic perspective: Russian policy in this area is driven by its hostility towards the United States, the Kremlin being keen to reduce the country's dependence on the major American platforms.

The pursuit of digital independence

The Russian authorities' fundamentally legalistic approach to the digital sphere reached its full expression in 2019 with the so-called "Sovereign Internet" law. The law's central feature was to provide Russia with a single "command and control" post from which authorities could manage the flow

75. J.-C. Plantin and G. de Seta, "WeChat As Infrastructure: The Techno-Nationalist Shaping of Chinese Digital Platforms", *Chinese Journal of Communications*, Vol. 12, No. 3, 2019, available at: www.tandfonline.com.
76. K. von Carnap, *et. al.*, "Fragmenting Cyberspace: The Future of the Internet in China", *op. cit.*, p. 33.
77. W. Cong, "The Spatial Expansion of China's Digital Sovereignty: Extraterritoriality and Geopolitics", *in* L. Belli and M. Jiang (eds), *Digital Sovereignty in the BRICS Countries*, Cambridge: Cambridge University Press, to be published in 2024.
78. A. Kokas, *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*, Oxford: Oxford University Press, 2022.
79. J. Nocetti, "Contest and Conquest: Russia and Global Internet Governance", *International Affairs*, Vol. 91, No. 1, 2015, p. 115.

of information in Russian cyberspace, including monitoring, limiting or blocking such flows across all or part of the Russian Internet. The law's provisions primarily cover two sectors: Internet traffic routing and control of the domain name system[80].

The latter is actually the result of a process first initiated a decade ago. When considering the creation of a "national" domain name system, the authorities were designing a system that would enable the Internet to continue to function even in the event of a split with the global Internet. Two processes have materialized since 2015; the first is the replication and takeover of the DNS coordination structures (registrar and registry), until then safe havens for the pioneers of the Russian Internet. The other was a series of tests conducted at the highest levels of the state to ensure RuNet's resilience should the Kremlin impose a digital shutdown in the event of a crisis – whether domestic (as a result of online activism taking to the streets) or foreign (in the event of cyber-attacks targeting Russia).

The first process redirects data flows to routing hubs operated by state-controlled actors[81]. These filter Internet traffic so that only data exchanged between individuals located in Russia reaches its destination. From a technical standpoint, all traffic in Russia must pass through government-approved Internet Exchange Points (IXPs).

Beyond network filtering for surveillance purposes, this strategy offers the possibility of disconnecting from the Internet in the event of external threats. The state has already demonstrated this system's effectiveness: in the fall of 2018, in response to protests in the Caucasian republic of Ingushetia over the revision of the border with neighboring Chechnya, the local FSB ordered local operators to cut off access to mobile networks in the Chechen Republic for two weeks[82]. The Kremlin expects the law to allow it to employ similar tactics remotely, by giving a command center in Moscow control over equipment to be installed at all ISPs, IXPs and border control points[83].

In practice, however, the highly distributed nature of the Russian Internet limits the extent to which a "sovereign Internet" could be effectively implemented, especially if complete disconnection is the goal[84]. This is nevertheless a step towards separation from the rest of the global network, given its degree of interdependence across national borders, and at every protocol layer. The Russian authorities' approach therefore closely

80. J. Nocetti, "Russia: A Narrow and Blurry Path Ahead", *in* A. Pannier (ed.), "The Technology Policies of Digital Middle Powers", *op. cit.*, p. 91.
81. K. Limonier, "Vers un 'Runet souverain' ? [...]", *op. cit.,* p. 45.
82. M. Kolomychenko, "Russia Stifled Mobile Network During Protests: Document", Reuters, November 16, 2018, available at: www.reuters.com.
83. J. Nocetti, "Le contrôle par la loi : les autorités russes et Internet", *in* S. Taillat, A. Cattaruzza and D. Danet (ed.), *La Cyberdéfense. Politique de l'espace numérique* (2nd edition), Paris: Armand Colin, pp. 220-222.
84. K. Limonier, "Vers un 'Runet souverain' ? [...]", *op. cit.*, p. 46.

combines the narrative – to defend against external threats – and the technical device that must seal off their means of connectivity *via* firm control over flows into and out of the Russian Federation.

War in Ukraine and fragmentation

The Russian invasion of Ukraine has stirred up fears of accelerated fragmentation of the Internet (and of the entire field of technologies underpinning the digital economy). This has manifested itself in various ways and across all Internet layers. Following the first round of Western sanctions aimed at isolating Russia from the world's main technology supply channels, Russia banned the major U.S. technology platforms from operating on its soil, before launching (or relaunching) Russian alternatives to Google Play and Instagram. This deliberate fragmentation was also put into effect by Western entities: the Firefox browser, for example, excluded the Russian Yandex from its search engine selection, and "Big Tech" made extensive efforts to technically remediate and support the fight against Russian disinformation to the benefit of Ukraine.

At the logical layer, Moscow's invasion of Ukraine involved the systematic rerouting of Internet networks in invaded regions, forcing their flows to pass through Russia. This data redirection not only delayed the flow of information, but also served to control and filter it, with the conquered Ukrainian regions now experiencing the world through the distorted prism of Russian censorship[85]. In this case, there is a direct relationship between the Internet's material architecture and the flow of information it produces, giving substance to the idea of the digital annexation of territories – which is only one aspect of the methods used to legitimize Russia's occupation of Ukraine[86]. In return, trying to block a large number of Russian Internet resources, the Ukrainian authorities have sought to structure an "informational shield" against Russia.[87]

Finally, at the start of the Russian invasion, Ukrainian and Western personalities approached ICANN to obtain the withdrawal or blocking of Internet addresses associated with Russia. The proposed measures included the temporary or permanent revocation of the .ru TLD, its Cyrillic equivalent (.рф), as well as .su; the withdrawal of authentication certificates from websites using these domain names; and the blocking of root servers located in Russia[88]. Then ICANN President Göran Marby rejected the request on the grounds that the Internet remains a decentralized system and "no one actor

85. M. Burgess, "Russia Is Taking Over Ukraine's Internet", *Wired*, June 15, 2022, available at: www.wired.co.uk
86. A. Satariano and S. Reinhard, "How Russia Took Over Ukraine's Internet in Occupied Territories", *New York Times*, August 9 2022, available at: www.nytimes.com.
87. L. Pétiniaud, "Le 'bouclier informationnel' ukrainien, une infrastructuration des pratiques de souveraineté numérique", *Réseaux*, to be published in 2024.
88. Discussions between the author and two experts involved in this petition to ICANN, February-March 2022.

has the ability to control or shut it down", as ICANN's role "does not extend to taking punitive actions, issuing sanctions, or restricting access against segments of the Internet – regardless of the provocations"[89].

India: partial fragmentation?

Recent international tensions – Sino-American rivalry, global disruption of commercial and technological supply chains, war in Ukraine – have accentuated the ambivalence of India's diplomatic standing, halfway between a "target" in the competition between Washington and Beijing, and a fast-emerging autonomous actor.[90] This ambivalence is reflected in India's position on Internet fragmentation.

Digital industry, data: in pursuit of sovereignty

While India is currently highly dependent on the United States and China for its equipment, software and platforms, digital sovereignty remains a stated objective for the government and is a pillar of its digital strategy, in the spirit of Prime Minister Modi's slogan *Atmanirbhar Bharat* ("Self-reliant India").[91]

In terms of e-government, the main project, India Stack, is composed of a set of open-source interfaces developed by the government that businesses may use to develop digital services. The most famous of these building blocks, the Aadhar system, provides each Indian with a unique identification number. India Stack also includes an identity verification tool (eKYC) and a payment system (UPI), which have contributed significantly to the development of the FinTech sector.[92] While these two projects do not "fragment" the global Internet *per se*, they are part and parcel of a more sovereign approach to the national digital space.

Despite technological interdependencies with the United States – India has become an "IT outsourcing superpower"[93] – New Delhi opposes initiatives aimed at the widespread liberalization of data transfers, in particular at the World Trade Organization (WTO). Several provisions require certain kinds of data to be stored and processed on Indian soil. The Reserve Bank of India's directive on data localization stipulates that all data relating to payment systems must be stored on servers located in India. The draft Data Protection Act proposes to generalize this requirement for all

89. G. Marby, "Letter to Ukrainian Minister of Digital Transformation Mykhailo Federov", ICANN, 2 March 2022, available at: www.icann.org.
90. T. Ray, "India: A Pivotal Player", *in* A. Pannier (ed.), "The Technology Policies of Digital Middle Powers", *op. cit.*, p. 31, available at: www.ifri.org.
91. A. Basu, "Sovereignty in a Datafied World", *Issue Briefs*, ORF, October 18, 2021, available at: www.orfonline.org.
92. On UPI, see V. Hariharan and S. Natarajan, "Digital Sovereignty and Payments: A Case Study of the National Payments Corporation of India", in L. Belli and M. Jiang (eds), *Digital Sovereignty in the BRICS Countries*, *op. cit.*
93. Author's interview, Paris, December 2023.

sensitive and critical data.[94] It should be noted that India's stance on data protection and localization is motivated more by economic rather than strategic goals, with the country's development objectives taking center stage in political discourse.[95]

Complex ties with U.S. and Chinese tech

New Delhi's regulatory policy has led to repeated disputes with U.S. digital platforms, in particular over access to encrypted data, content moderation and the business environment. The 2021 Digital Media Ethics Code thus requires platforms to be able to trace the origin of messages and filter their content. This undermines the end-to-end encryption model implemented by companies like WhatsApp, which brought the case before the Delhi High Court in 2021[96]. Disputes also emerged over content regulation issues. In 2021, again, the Indian government requested that Twitter block certain accounts in connection with farmers' protests. According to the government, these accounts were guilty of "disseminating false information" and threatening "national security", but the firm refused[97]. In response, many BJP party officials and executives switched from Twitter to Koo, a competing local platform.

These conflicts with Big Tech firms sometimes affect inter-state relations. India's proposed tax on digital services was initially criticized by the White House as discriminating against U.S. companies – before a favorable outcome was reached after bilateral talks.[98]

When a crisis erupted between Beijing and New Delhi in May 2020, Indian authorities blocked 59 Chinese applications, citing national security risks. The list has gradually grown to include more than 200, including WeChat, AliExpress and TikTok. In the telecommunications sector, Huawei and ZTE have been excluded from 5G network test phases. Chinese smartphone manufacturers, for their part, have been required to provide a list of their products' components and the data they store. These measures severely limit Chinese companies' ability to expand into the Indian market.

94. N. Mishra, "Digital Governance and Digital Trade in India: Losing Sight of the Forest for the Trees?", *in* A. Chander and H. Sun (eds), *Data Sovereignty: From the Digital Silk Road to the Return of the State*, Oxford: Oxford University Press, 2023, pp. 249-253.
95. *Ibid.*, p. 263.
96. See T. Derivry, "La souveraineté numérique en Inde : programme politique, discours, pouvoir et capacité d'action", Sciences Po, Digital, Governance and Sovereignty Chair, May 9, 2023, available at: www.sciencespo.fr.
97. S. Phartiyal, "India to Twitter: Comply with IT Rules or Face 'Unintended Consequences'", Reuters, June 5, 2021, available at: www.reuters.com.
98. "USTR Welcomes Agreement with India on Digital Services Taxes", Office of the United States Trade Representative, November 24, 2021, available at: https://ustr.gov/.

Ambivalence in international negotiations

India's position in Internet governance forums reflects the contradictions certain countries face in attempting to carve out a "third way" between a multistakeholder model, which is sometimes criticized for its lack of legitimacy and representativeness, and a multilateral, UN-style model based on state sovereignty. Indeed, New Delhi's posture fluctuates, in an attempt to combine increased connectivity and digital sovereignty.[99] While India's political discourse shows a commitment to the rhetorical framework of the BRICS, with a more tangible post-colonial slant than in other member countries, India stands out among the other major emerging countries for its proximity, both economically and in terms of security, to the United States. India's close ties with the Silicon Valley ecosystem give the country's major private players (Infosys, Wipro, etc.) considerable political clout. This, combined with the aspirations of a substantial proportion of the country's connected youth, means that Delhi's positions in bodies such as the Internet Governance Forum (IGF), ICANN's Governmental Advisory Committee (GAC), the UN's Open-Ended Working Group, and events such as the Sao Paulo NETmundial in 2014, remain largely elusive.[100] This ambivalence is seen by some as a simple quest for osmosis between the expected dividends of opening up to foreign technology and capital, and security considerations that have become more entrenched within the state apparatus.[101]

European Union: the pursuit of "digital sovereignty" without Internet fragmentation

Internet fragmentation is rarely addressed within the European Union, which is now the leading producer of legal standards intended to provide a global framework for a digital economy dominated by the Sino-American duopoly. Most debates are framed in a dual economic and legal perspective, which forms the basis of Europe's "digital sovereignty" ambitions.

Legislation trumps "fragmentation"?

As relations in the global digital arena grow tenser, the European Union has until now distinguished itself as a "regulatory superpower".[102] This penchant

99. J. Nocetti, "Puissances émergentes et internet [...]", *op. cit.*, p. 50.
100. *Ibid.* See also A. Barrinha and R. Turner, "Strategic Narratives and the Multilateral Governance of Cyberspace: The Cases of European Union, Russia, and India", *Contemporary Security Policy*, October 2023 (online), p. 17, available at: www.tandfonline.com; M. Kaul, "Global Internet Governance: India's Search for a New Paradigm", *ORF Issue Brief*, ORF, No. 74, August 2014, available at: www.orfonline.org.
101. S. Mohan, "Practising Digital Osmosis: India's Role in the Global Splinternet", ORF, February 7, 2023, available at: www.orfonline.org.
102. A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford: Oxford University Press, 2020.

for standard-setting on the international stage is not new to EU politics: it underscores what remains the EU's major (geo)political resource, namely its ability to produce and deploy a broad array of standards at the global scale.[103] Anu Bradford describes this "Brussels effect", as it applies to the digital sphere, as the EU's ability to extend its influence on international markets by leveraging its normative power to shape the personal data policies of non-European technology platforms and states.[104]

The EU's digital standards strategy reflects unambiguous legal ambitions, mobilizing extraterritorial instruments. A plethora of institutional and legal publications began to appear in 2020: the White Paper on Artificial Intelligence (February 2020), the "Digital Compass" (June 2021), the 5G "Toolbox" (2020), the Data Strategy, the Digital Markets Act and the Digital Services Act (2023), the Digital Education Action Plan 2021-2027, the FinTech Action Plan, the Cybersecurity Act, the AI Act, the Blockchain Regulatory Sandbox, etc. It should be noted that some of these texts, such as the one on 5G, are non-binding.

The European Union's strong emphasis on law is thus evident, drawing on its internal market law and the principles and values laid out in European treaties. The objective for Brussels is to give legal expression to its political ambitions, with the main goal, since 2019, being to introduce, for each major theme of the digital sector, a corresponding major European Act, a European law recognizable the world over, treating the extraterritoriality of its legislation as a matter of course.[105]

The EU thus seems to be developing a brand of digital diplomacy which makes no secret of its unilateralism, by leveraging the global reach of European regulation. The Global Digital Compact, a United Nations initiative intended to define common principles for the future of the Internet, due to be discussed in September 2024, has been the subject of a EU Council memorandum focusing in part on the need to prevent the technical, economic and geopolitical fragmentation of the Internet.[106]

Towards strategic autonomy through infrastructure? The DNS4EU project

The European DNS resolver project, mentioned in the European Union's Cybersecurity Strategy for the Digital Decade,[107] was formally launched in January 2022. There are two categories of DNS servers: authoritative

103. *Ibid*.
104. A. Bradford, *Digital Empires: The Global Battle to Regulate Technology*, Oxford: Oxford University Press, 2023, pp. 324-326.
105. B. Bertrand (ed.), *La Politique européenne du numérique*, Brussels: Bruylant, 2022.
106. "European Union Contribution to the Global Digital Compact", March 2023, available at: www.un.org.
107. "The EU's Cybersecurity Strategy for the Digital Decade", European Commission, December 14, 2020, available at: https://digital-strategy.ec.europa.eu/.

servers, which store data retrieved via the DNS protocol; and resolvers, which are the servers directly queried by terminals. The DNS4EU initiative aims to respond to both the exponential consolidation of the DNS resolver market and the proliferation of digital risks (cyber-attacks, outages). In the industry, non-European actors (Google, Cloudflare) dominate the market of so-called open resolvers.[108]

From a technical standpoint, DNS4EU will have to comply with existing legal provisions, including filtering requirements for web addresses containing illegal content (terrorism propaganda, child pornography, piracy, etc.). DNS4EU aims for maximum accessibility and compatibility between terminals and operating systems, in particular in terms of security and privacy standards, as well as with the IPv6 protocol. In addition to being a step towards European "strategic autonomy" in technological terms, DNS4EU is Brussels' most notable intervention in a largely privatized market driven by consumer choice.[109] Although the project has not seen any significant steps in its development since, DNS4EU is due to be deployed by the end of 2025.

Solving the market/security equation for DSN4EU, as spelled out in the EU Cybersecurity Strategy, essentially addresses issues raised in other documents published by European institutions, such as the Directive on the Resilience of Critical Entities and the NIS-2 Directive.

The European Union's work on Internet infrastructure also has a diplomatic dimension. The "Global Gateway" initiative presented by the European Commission in December 2021 contains a series of commitments to invest in so-called connectivity infrastructure – similar to China's New Silk Roads project – including digital infrastructure such as submarine and terrestrial fiber-optic cables, secure satellite communication systems and cloud infrastructure. In this context, EU investment will be tied to "standards and protocols that support network security and resilience, interoperability and an open, plural and secure Internet".[110] The European Union is thus pursuing a policy aimed precisely at countering the global trend towards fragmentation in the field of telecommunications and digital technologies.

108. 20% of global Internet traffic relies on open resolvers. See A. Durand, "DNS Resolvers Used in the EU", ICANN, March 1, 2022, available at: www.icann.org.
109. R. Radu, "DNS4EU: A Step Change in the EU's Strategic Autonomy?", *Journal of Cyber Policy* (online), December 2023, available at: www.tandfonline.com.
110. "The Global Gateway", Joint Communication to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank, European Commission, December 1, 2021, available at: https://eur-lex.europa.eu/.

Conclusion

While the Internet's continuity initially ensured a form of deterrence – interdependence and connection to a shared network guaranteeing mutual vulnerability –, its current compartmentalization into "national" networks by authoritarian states is likely to continue to exacerbate the instability of cyberspace. As these states' ability to protect their networks from accidental repercussions[111] or retaliation grows, so will the temptation for them to attack their adversaries directly.

The consolidation of data flows in the hands of a few central routing entities (the Big Five tech giants in particular) also threatens the global continuity of web services, as evidenced by Facebook's major outage. In October 2021, the social network and its subsidiaries (including WhatsApp and Instagram) experienced a worldwide outage lasting over seven hours, caused by the loss of IP routes to Facebook's DNS servers. While also encouraging these gatekeepers to exercise greater responsibility, the goal should be to promote the decentralization and global diversification of routing. This "commercial" dimension of fragmentation requires greater attention, though the emphasis is more often placed on the geopolitical intentions of states.

In this regard, China's dual approach to the development of Internet standards (a mix of cooperation and fragmentation), Russia's ambitions to redesign its Internet infrastructure, and India's apparent ambivalence all illustrate the ways in which states have increasingly adopted strategic approaches in dealing with the Internet and its standards.[112] The European Union and its specific approach, patiently building consensus and betting on the export of its laws, stands in contrast to these three countries, resisting the centrifugal forces at work in the digital arena. The United States, for its part, is committed to preserving its technological dominance – starting with the Internet – and is adapting its traditional approach, combining technological openness, innovation and the democratization of societies, to pursue a more coercive strategy focusing on China.

The concept of fragmentation helps to highlight such important issues in the digital field, which have real repercussions for users. Yet it is not without its ambiguities: the term has been applied in political discourse to everything from the domain name system to net neutrality, online censorship

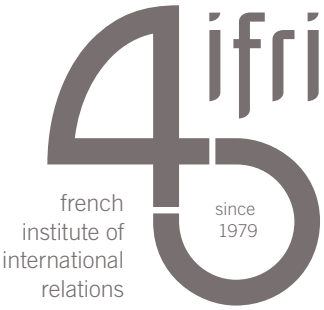
111. As with the NotPetya cyberattack in 2017, launched by Russian operators against Ukrainian networks, whose runaway propagation ended up affecting computer systems in Russia.
112 C. Perarnaud, *et. al.*, "'Splinternets' [...]", *op. cit.*, p. 45.

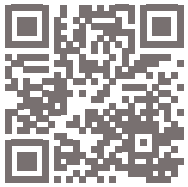
and various privacy protection systems, leading to confusion, in particular in the United States.

The nuances of digital capitalism challenge the coexistence of the different models that exist: Silicon Valley's "open Internet", Washington's "commercial Internet", China's "paternal Internet" and Brussels' "bourgeois Internet"[113] all have their own distinct philosophical, legal and economic specificities. Whether as the foundation or a mirror of an already fragmented international system, the Internet may be exposed to perpetual instability, a reality that will have to be managed while preserving the benefits it offers.

During the 2010s, fragmentation was the subject of much debate, though primarily among experts. It also largely focused on the risks specific to DNS. Since then, a plethora of geopolitical and commercial developments, among others, have made the prospect of fragmentation more tangible, even systemic, as the issue of Sino-American technological "decoupling" clearly reflects.

113. This is the taxonomy adopted by K. O'Hara and W. Hall in *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