Governing the Internet for the Global Common Good: A Roadmap for the G20 and G7

Hagebölling, David; Weber, Valentin; Meinel, Christoph; Barker, Tyson

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Governing the internet for the global common good

A roadmap for the G20 and G7

Policy brief

Authors:

David Hagebölling
Research Fellow,
Hasso Plattner Institute
for Digital Engineering &
German Council on Foreign
Relations

Valentin Weber
Research Fellow,
German Council on
Foreign Relations

Christoph Meinel
Scientific Director and CEO,
Hasso Plattner Institute for
Digital Engineering

Tyson Barker
Head of Technology and
Global Affairs Program,
German Council on
Foreign Relations

Institutions:

The Hasso Plattner Institute (HPI) in Potsdam is Germany's university center of excellence for digital engineering. With its Bachelor's and Master's degree programs in "IT Systems Engineering", the Digital Engineering faculty at the University of Potsdam offers a unique and particularly applied computer science degree program throughout Germany. In the CHE university rankings, HPI consistently occupies top positions. The HPI School of Design Thinking is also Europe's first innovation school for students modeled on the Stanford d.school and research schools on all continents.

Social media:
Twitter: @HPI_DE
Facebook: facebook.com/hassoplattnerinstitute
LinkedIn: linkedin.com/school/hasso-plattner-institute

Keywords:
Global Governance; Internet Fragmentation; Digital Infrastructure; Cybersecurity; G7/G20

The German Council on Foreign Relations (DGAP) is committed to fostering impactful foreign and security policy on a German and European level that promotes democracy, peace, and the rule of law. Since its founding in 1955, the nonpartisan organization's members and research have continued to shape the debate on foreign policy issues in Germany. DGAP's experts provide decision-makers in politics, business, and civil society with strategic advice based on their foreign policy research and train young professionals in international leadership programs.

Social media:
Twitter: @dgapev
Facebook: facebook.com/dgapev
LinkedIn: linkedin.com/company/german-council-on-foreign-relations

INTRODUCTION

The internet is the backbone of our digital world. It creates the conditions for economic development and prosperity worldwide. Yet, this critical common good – the open, global, and trustworthy internet – is under threat. As digital connectivity penetrates every aspect of economic, political, and social life, it has become a central object of geopolitical maneuvering. Amid the heightened competition between the United States and China and a push towards greater "digital sovereignty" by the European Union, India, Russia, Turkey, and other players – the meaning of which varies greatly –, regulatory divergence, increasing tensions in cyberspace, political disinformation, and surveillance hamper the free flow of information. Private power on the internet has also concentrated to an unprecedented degree, undermining economic competition and dominating governance institutions.

Even more concerning is that geopolitics are trickling down from the upper layers of internet usage to the internet's underlying infrastructure. Whereas issues such as data privacy, surveillance and platform regulation are at the top of policymakers' agendas, the daunting prospect of a fundamental splintering of the internet along national borders down to its very core demands serious and immediate attention. And yet, the internet's physical (e.g., submarine cables) and logical (e.g., TCP/IP protocol family, DNS) infrastructure represents its foundation as a "network of networks" that enables any device to exchange data packets with any other device worldwide. A splintering of this infrastructure would be difficult to reverse.

Preserving an open, global, and trustworthy internet infrastructure must thus be a priority for global leaders. The technical bodies that govern the internet are currently ill-equipped to address the political fault lines that put the global internet at risk. The G20 and G7 should actively work to mitigate these political fault lines so that technical bodies can continue to effectively administrate and develop an internet that works for the global common good.

A GLOBAL COMMON GOOD CAUGHT IN POLITICAL CROSSFIRE

Fragmenting the internet at the infrastructural level would effectively dismantle the digital roads that enable global economic growth and development. Global e-commerce in 2019 amounted to no less than USD 26.7 trillion.[1] A series of temporary internet shutdowns have cost the global economy an estimated USD 16.9 billion since 2019.[2] Modern transnational supply chains and business operations depend heavily on the ability to exchange data freely and securely. Worryingly, developing countries are likely to be hit hardest by the negative effects of internet fragmentation. Their integration in global supply chains and access to foreign markets – both heavily dependent on digital connectivity – are primary sources for investments and economic growth.

Internet fragmentation also has wider scientific, political, and social consequences. Fragmentation would roll back interactions that further technological innovation and scientific advancement and were once at the heart of the public internet's origins as a network linking research institutions and universities. In the same vein, responses to global challenges such as pandemics depend on unhindered and frictionless global information flows among scientific communities and public institutions. Finally, and most importantly, people's ability to connect transnationally, build mutual understanding, and express their opinions freely would be severely curtailed.

HOW GEOPOLITICS IS TRICKLING DOWN TO THE INTERNET'S CORE

Physical communications infrastructure

At the most fundamental level, the internet connects users through a network of undersea cables. Even as companies are making a significant push into satellite technologies to provide internet access even to remote and underserved locations on the globe, cables will remain the main pipelines of cyberspace for the rest of the 2020s. Today, an estimated 436 undersea cables transport approximately 99 percent of all international traffic.[3] International communications and the global economy depend on them.

However, the physical communications infrastructure that the internet uses is on the verge of a paradigm shift. Concerns about the insertion of backdoors and surveillance at landing stations and fears of sabotage render these cables' construction, operation, and geography politically salient. Since the Snowden revelations, trust in global internet traffic has taken a hit, and submarine cables have received increasing attention as a geopolitical factor. Brazil reacted by pushing ahead on an undersea cable that would connect it directly to Europe and reduce the risk of man-in-the-middle snooping from the US.[4] This EllaLink cable was launched in mid-2021 and is the first of its kind between the two continents.[5]

The physical communications infrastructure is also moving to the center of the US-China rivalry.[6] Chinese and US companies are rapidly growing their market share. By 2018, Amazon, Facebook, Google, and Microsoft alone already owned or leased more than half of the world's undersea bandwidth.[7] Huawei Marine Networks (now rebranded as HMN Technologies) has become one of the biggest vendors in the submarine cable market.[8] European companies are also represented among the major players that operate global submarine cables, including Alcatel Submarine Networks, Nexans Norway AS, NKT A/S, and Prysmian Group.[9] As a result, the privately owned and operated internet infrastructure is ripe for the projection of geopolitical tensions. Lately, Huawei's participation in the "Peace Cable", running from China to France, has led to intense US pressure on European partners to abort participation.[10] Last year, US authorities recommended blocking a 12,800-kilometer cable connecting the US and Asia, built in a partnership between Google, Facebook and other companies.[11] What will be the "highest-capacity trans-Pacific route"[12] ever built will now link to Taiwan instead of Hong Kong.[13] It is the first time that a planned undersea cable connection to mainland China has been rerouted in response to national security concerns.

Internet communications protocols

Even as the physical infrastructure is only beginning to align with geopolitical fault lines, the communications protocols that underpin the global internet are already at the center of political contestation. The internet's communications protocols are placed on top of the physical cables and satellites that connect devices. They encompass the technical protocols, notably the Transmission Control Protocol/Internet Protocol (TCP/IP) family of network protocols, regulating how devices communicate as well as the Domain Name System (DNS), the internet's address book. In addition to these, cryptographic protocols, such as Transport Layer Security (TLS), which ensure the secure transmission of data, are essential building blocks to a trustworthy internet.[14]

»The internet is the backbone of our digital world.«

Internet communications protocols are already part of the drive for a nation-state-organized internet. Russia is building a national DNS to be able to handle requests autonomously.[15] With "NewIP", a Chinese company (Huawei) introduced an initiative to revamp the current internet protocol family.[16] While oriented towards developing protocols with a view to the rapidly evolving requirements of a future internet, it would link internet protocols in ways that would make it easier for actors, including governments, to monitor and control communication flows.[17] The critique voiced about TCP/IP within the argumentation for NewIP is unsubstantiated, and despite possible unilateral moves, widespread adoption may

be difficult, not least due to the expensive nature of protocol migrations that are slowing the migration from IPVv4 to IPv6.[18] Yet, while the controversy around NewIP is currently stalled in the International Telecommunication Union, there is an acute risk that states will pursue the adoption of preferred protocols unilaterally where no viable agreement can be reached. Indeed, an alternative vision of the internet is already being tested within China but may well be rolled out through outbound infrastructure investments, especially in developing countries.[19]

The internet is also at risk of further fragmentation because states starkly vary in how strongly they implement cryptographic protocols. In some parts of the world, implementation of key protocols is lagging or outright opposed, undermining secureness to facilitate greater surveillance over domestic populations. TLS 1.3 and Encrypted SNI are crucial to preserving the anonymity and privacy of internet users across the world. At the same time, they make it harder for states to know what web pages citizens are viewing. Therefore, China and Russia have restricted their implementation domestically.[20] This contrasts with the US, UK and the EU, which rely on strong and ubiquitous cryptographic protocols.

»Even more concerning is that geopolitics are trickling down from the upper layers of internet usage to its underlying infrastructure.«

Therefore, it is concerning that the US, UK and the EU have also signaled that they aim to weaken end-to-end encryption (E2E) for national security reasons. If they were moving ahead with their announcements, it would severely weaken the internet's trustworthiness.[21] This is because there is no technical way to undermine E2E encryption that would only allow law enforcement access to messages that are E2E encrypted. Any weakening of encryption protocols also means an increased risk of criminals using the same vulnerabilities. Updating cryptographic protocols used on the internet is essential since it ensures the privacy and anonymity of users. At the same time, it protects states from snooping or malicious activity by other state actors or cybercriminals.[22]

REVIVING MULTISTAKEHOLDERISM IN 21ST CENTURY INTERNET GOVERNANCE

The institutions that govern the internet currently struggle to address these challenges to the world's digital nervous system. Multistakeholderism is deeply engrained in the internet's origins. In this model, players from the technical community, business, civil society, and governments jointly drive forward the development of the internet in specialized institutions, usually based on "rough consensus". The Internet Engineering Task Force (IETF), for example, establishes protocols and standards. The Internet Corporation for Assigned Names and Numbers (ICANN) manages central functions such as the DNS mentioned above. The Internet Society (ISOC), a non-governmental organization, forms the focal point for coordinating the maintenance and further development of the internet.[23]

These institutions have demonstrated an exceptional capacity to develop and administer the internet technically, but they stand unprepared for the geopolitical pressures that are now building up. Institutions like the IETF, which came to life when the internet was under development, was mainly the concern of a technocratic community of computer scientists and engineers. Today, technical decisions have significant political implications. Yet, there is currently no functioning mechanism for bridging technical and political considerations. The Internet Governance Forum (IGF), created precisely to structure dialogue among all stakeholders – from government to civil society – has so far failed to develop the focality and authority to mitigate tensions among parties and inform internet governance. As a result, political frictions are not channeled into productive deliberations among concerned stakeholders but translated into institutional powerplay. The NewIP proposal is a case in point, with its proponents attempting to shift internet development from the multistakeholder IETF to the intergovernmental ITU.[24]

The lack of an adequate political process and institutional powerplays are damaging the prospects of retaining an effective ecosystem to develop and administer an internet that remains open, global and trustworthy. A clear division of labor among governance bodies – fundamental to a well-functioning governance ecosystem – is being eroded. Within institutions as well, fault lines are becoming more entrenched. The 2022 elections of a new ITU Secretary-General are descending into a geopolitical haggling between those that defend a limited role of the ITU and those that seek its transformation into a centralized and intergovernmental internet decision-making body.[25]

»Digital geopolitics is proving a potent destabilizing force to internet governance.«

Digital geopolitics is proving a potent destabilizing force to internet governance because it preys on multistakeholder institutions' lack of inclusion and representativeness. Internet institutions like the IETF and ICANN were created mainly throughout the 1980s and 90s. At that time, the internet was very US-centric. In fact, the US Department of Commerce's oversight over ICANN and its functions was only removed as late as 2016.[26] China and Russia, major cyber powers today, occupied only marginal positions in internet governance at the time.

Since then, the internet has changed significantly. Most of today's internet users are situated outside of Western industrialized countries.[27] China alone boasts over a billion internet users.[28] At the same time, internet governance institutions have adapted slowly. Organizations like ICANN

and ISOC remain domiciled in the United States and are subject to US and, in the case of ICANN, California state law.[29] The IETF's leading figures are employed by Western companies and universities.[30] In that sense, the internet institutions were never genuinely global – a deficit that is becoming more severe every day that the internet expands.

Multistakeholderism, which originated in a close-knit community of technical experts and academics, is also struggling with the concentration of power in the hands of few actors, particularly private companies. A key strength of internet governance institutions is their techno-

»Preserving an open, global, and trustworthy internet infrastructure must be a priority for global leaders.«

cratic nature and focus on devising the best possible technical (as opposed to political) solution. On the flip side, active engagement consumes expertise, time, and capital that is disproportionally in the hands of dominant technology companies. Their involvement is essential, but the lack of broader geographical and civil society representation, including from developing countries, fuels the contestation of multilstakeholderism and creates incentives to flock to an alternative state-centric and multilateral model. Moreover, multistakeholder formats can give rise to unrepresentative, insular communities that exclude new entrants.

Internet governance institutions like the IETF and ICANN have shown their exceptional capacity to administer one of the fastest growing and most complex infrastructures in human history. Preparing for the coming decades, however, will require a process of reform that is unlikely to come from within alone. Governments thus have a constructive role to play in working with multistakeholder institutions to increase their global inclusion and representativeness as the next billion users come online.

RECOMMENDATIONS TO THE G20 AND G7

The G20 should take action in the following areas:

– **Global internet opportunities:** emphasize that an open, global, and secure internet is a critical enabler for inclusive economic growth and addressing global challenges, including those laid out in the UN Sustainable Development Goals.

– **Inclusive multistakeholderism:** reaffirm its support for complementing multilateral engagement on digital cooperation with an inclusive multistakeholder approach, involving civil society, academics, businesses, and governments, echoing the recommendations of the UN High-level Panel on Digital Cooperation.

– **Physical infrastructure integrity:** declare their ambition to initiate a multistakeholder dialogue on ways to increase the trustworthiness of physical infrastructure (i.e. undersea cables) in the interest of advancing global connectivity.

– **Interoperability by design:** limit public funding to domestic and international digital infrastructure investments that retain compatibility with the globally used protocol family (i.e. TCP/IP) and global DNS by design.

– **Internet Governance Forum "Plus":** define concrete steps to strengthen the Internet Governance Forum (IGF), drawing on the follow-up recommendation to the UN Secretary General's initiative for strengthening global digital cooperation (IGF "Plus").

– **Human-centric digital connectivity:** agree to expand investment in digital connectivity in the Global South while committing to protect users' privacy and rights, including freedom of expression, from overreach by both businesses and governments.

In view of the above, the G7 should lead by example with actions in these areas:

– **Inclusive multistakeholder governance:** reaffirm its commitment to inclusive multistakeholder governance of the internet and pledge to provide funds supporting the technical community and civil society representatives from the Global South.

– **Digital human rights:** pledge their joint support for a secure and trustworthy internet that strengthens digital human rights, notably by refraining from undermining end-to-end encryption and fostering the fast roll-out of the latest cryptographic protocols, such as TLS 1.3 and Encrypted SNI.

1 https://unctad.org/press-material/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-retail-sales

2 https://www.top10vpn.com/cost-of-internet-shutdowns/

3 https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions

4 https://world.time.com/2014/02/24/brazil-plans-underseas-cable-to-europe-to-avoid-u-s-snooping/

5 https://eeas.europa.eu/delegations/chile/99293/eu-and-lac-come-together-6000-km-high-capacity-submarine-cable-bridges-digital-gap-between-two_ka

6 https://www.swp-berlin.org/publikation/cracks-in-the-internets-foundation

7 https://internethealthreport.org/2019/the-new-investors-in-underwater-sea-cables/

8 https://subtelforum.com/hengtong-set-to-shape-the-global-subsea-market/

9 https://www.coherentmarketinsights.com/market-insight/submarine-cables-market-4300

10 https://www.bloomberg.com/news/articles/2021-03-05/china-s-peace-cable-in-europe-raises-tensions-with-the-u-s

11 https://www.bbc.com/news/world-asia-53088302

12 https://cloud.google.com/blog/products/gcp/new-undersea-cable-expands-capacity-for-google-apac-customers-and-users

13 https://www.datacenterknowledge.com/google-alphabet/google-facebook-dump-plans-us-hong-kong-undersea-cable

14 https://link.springer.com/book/10.1007/978-3-540-92940-6

15 https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law

16 https://www.huawei.com/de/deu/magazin/aktuelles/new-ip

17 https://www.tandfonline.com/doi/full/10.1080/23738871.2020.1805482

18 https://www.internetsociety.org/resources/doc/2020/discussion-paper-an-analysis-of-the-new-ip-proposal-to-the-itu-t/

19 https://www.scmp.com/news/china/science/article/3130338/china-starts-large-scale-testing-its-internet-future

20 https://www.lawfareblog.com/how-chinas-control-information-cyber-weakness

21 https://www.eff.org/deeplinks/2020/10/orders-top-eus-timetable-dismantling-end-end-encryption

22 https://www.lawfareblog.com/how-chinas-control-information-cyber-weakness

23 https://dgap.org/de/forschung/publikationen/internet-governance

24 https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf

25 https://www.washingtonpost.com/politics/2021/10/12/us-russian-candidates-both-want-lead-un-telecom-arm/

26 https://www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana

27 https://www.itu.int/en/ITU-D/Statistics/Pages/stat/Treemap.aspx

28 https://www.cnbc.com/2021/02/04/china-says-it-now-has-nearly-1-billion-internet-users.html

29 https://www.theguardian.com/technology/2016/mar/14/icann-internet-control-domain-names-iana

30 https://www.icann.org/locations
https://www.ietf.org/about/groups/iesg/members/
https://www.ietf.org/about/administration/llc-board/