SWP

SWP Research Paper

Daniel Voelsen

Cracks in the Internet's Foundation

The Future of the Internet's Infrastructure and Global Internet Governance

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

SWP Research Paper 14
November 2019, Berlin

The foundation of the Internet is showing cracks. Central elements of the Internet's infrastructure are the result of decisions made decades ago. Since then, however, the technical context has changed dramatically, as has the political significance of the Internet.

Three conflicts over the future development of the Internet infrastructure are particularly important for German policy-makers. The first is about security and privacy in the Internet's addressing system, the so-called Domain Name System (DNS). Second, a conflict is building up over the security of the Border Gateway Protocol (BGP) — the protocol used to coordinate data traffic on the Internet. Third, the security and availability of submarine cables, which form the physical backbone of the global Internet, are proving increasingly problematic.

If these conflicts remain unresolved, while at the same time the demands on the Internet continue to rise worldwide, the consequences for security, privacy, and economic development will be increasingly negative. Moreover, the Internet is in danger of being split, all the way to the infrastructure level.

This multifaceted field of conflict demands a clear strategic approach from German policy-makers. In accordance with their own digital policy demands, they should at the same time pursue the goal of worldwide interoperability and address the issues described within a European framework. The challenge here is to shape the further development of the Internet infrastructure in Europe in such a way that it complements — and does not further jeopardise — the shared global foundation of the Internet.

SWP Research Paper

Daniel Voelsen

Cracks in the Internet's Foundation

The Future of the Internet's Infrastructure and Global Internet Governance

Stiftung Wissenschaft und Politik
German Institute for International and Security Affairs

SWP Research Paper 14
November 2019, Berlin

SWP Research Papers are
peer reviewed by senior
researchers and the execu-
tive board of the Institute.
They are also subject to fact-
checking and copy-editing.
For further information
on our quality control pro-
cedures, please visit the
SWP website: https://
www.swp-berlin.org/en/
about-swp/quality-
management-for-swp-
publications/.
SWP Research Papers reflect
the views of the author(s).

SWP
Stiftung Wissenschaft und
Politik
German Institute
for International
and Security Affairs

Ludwigkirchplatz 3—4
10719 Berlin
Germany
Phone +49 30 880 07-0
Fax +49 30 880 07-200
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1863-1053
doi: 10.18449/2019RP14

(English version of
SWP-Studie 12/2019)

Table of Contents

5 Issues and Recommendations

7 Internet Governance As a Task for German Policy-makers
7 Governance
7 Tasks and Goals of German Policy-makers

10 The Current Model of Internet Governance
10 Global Standards
11 Authoritative Rule-setting by ICANN
12 Legitimacy through Multi-stakeholder Governance

14 Conflicts over the Global Infrastructure of the Internet
15 Security and Privacy in the Domain Name System (DNS)
16 Security in the Routing System
18 Security and Availability of Submarine Cables

22 Authoritative Rule-setting As a Way Out?
22 ICANN: Politicisation
24 ITU: Blockade

27 Two, Three, Multiple Internets?

30 Recommendations for German Internet Governance Policy
30 The Strategic Context
31 Priorities
31 Restricting ICANN to Its Core Technical Functions
33 Public Support for Multi-stakeholder Institutions in the ITU and the IGF
33 Updates to the Internet Infrastructure on the European Level

35 Abbreviations

Dr Daniel Voelsen is an Associate in the Global Issues Division at SWP

Cracks in the Internet's Foundation. The Future of the Internet's Infrastructure and Global Internet Governance

The lifestyle of modern societies is increasingly dependent on the exchange of information via the Internet. This is especially true for the economy, but increasingly also for state institutions. Reports on the political and economic consequences of hacker attacks clearly illustrate how indispensable the Internet has become for public and private institutions — and how vulnerable they are.

The focus is usually on institutions threatened by attacks. In contrast, the infrastructure of the Internet is hardly considered in this context. A multitude of protocols and standards, together with the physical network of cable connections and routers, form this infrastructure — and thus the global foundation of the Internet. Originating in the United States, this infrastructure developed worldwide in the course of the 1990s, and with it the no-less-complex institutional network of global Internet governance.

Increasingly, however, cracks are appearing in the foundation of the Internet. Central elements of the infrastructure are the result of decisions made decades ago. Since then, the technical context has changed dramatically, as has the political significance of the Internet. In light of the goals that German policymakers have set for themselves, three conflicts over the Internet infrastructure are of particular importance.

The first concerns the security of the Domain Name System (DNS), that is, the technical system for assigning domain names and IP addresses. Configurations that once made sense now lead to serious security gaps and create simple ways to violate the privacy of Internet users. There are mature proposals for solutions to these problems, but they cannot be implemented in the existing Internet governance structures.

Secondly, there is a conflict over the security of the routing system. The Border Gateway Protocol (BGP) provides the technical means to coordinate the transport of data within the decentralised structure of the Internet. In recent years, however, there has been an increasing number of cases in which states and private actors have used this protocol to manipulate data

traffic on the Internet. Here, too, solutions exist that are not being implemented.

Thirdly, the security and availability of submarine cables are proving to be increasingly problematic. The majority of these cables are operated by private companies, whose planning understandably is based on economic criteria. The consequence, however, is that individual routes and landing points are frequently reused — resulting in particularly vulnerable "choke points". Moreover, many developing countries are insufficiently connected to the global submarine cable network. In this respect, a largely overlooked conflict exists between the security interests of the states and the interests of the companies involved.

If these conflicts remain unresolved, while at the same time the demands on the Internet continue to rise worldwide, this will have increasingly negative consequences for security, privacy, and economic development. In addition, the conflicts point to a systemic problem of global Internet governance. Non-state actors, above all private companies, have a formative influence here. They provide important public goods in the form of protocols and standards, but they have neither the economic incentives nor the necessary legitimacy to bring political conflicts to an end through authoritative rule-making. Even where technically mature solutions are available, the Internet infrastructure is therefore not being developed in the necessary way.

In principle, two institutions could fill this gap: the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Telecommunication Union (ITU). On closer inspection, however, both prove to be ill-suited. The current political controversies surrounding ICANN show that the organisation does not have the necessary legitimacy to set authoritative standards beyond a limited technical scope. Although this aspect is less of a problem for the ITU as a specialised agency of the United Nations, there is fundamental dissent among the member states of the institution on issues of Internet governance, which is why the ITU has been blocked on this issue for a long time and will probably remain so for the foreseeable future.

Against this background, the concern about a possible fragmentation of the Internet becomes particularly acute. At the level of Internet services, regulatory fragmentation along national borders is already a practical reality. The crucial question, however, is whether this fragmentation will propagate to the level of the Internet infrastructure. The inability of today's institutions to solve the problems of the global Internet infrastructure creates a breeding ground for this. Companies such as Google and Mozilla already offer their own DNS services. China and Russia have also repeatedly signalled their interest in setting up an alternative infrastructure. There is thus a growing danger that the cracks in the foundation of the Internet will turn into genuine fractures.

This conflict situation demands a clear strategic orientation from German policy-makers. In line with the goals set by German policy-makers themselves, they should simultaneously pursue the goal of global interoperability and address the problems described within a European framework. The non-trivial challenge here is to shape the further development of the Internet infrastructure in Europe in such a way that it complements — and does not further jeopardise — the common global foundation of the Internet.

These objectives can be translated into three recommendations for German policy-makers. The first is to work towards limiting ICANN to those core technical functions that are necessary for the operation of the DNS. A unified DNS is essential to the goal of global interoperability, and it is in this area that ICANN's authority is widely recognised. Second, German policy-makers should use their influence in the ITU and the Internet Governance Forum (IGF) to provide support to multi-stakeholder institutions wherever they make important contributions to the technical development of the global Internet infrastructure. Third and finally, Germany should make every effort to tackle within the European Union (EU), as far as possible, those problems of this infrastructure that cannot currently be solved at the global level. This should be done out of a well-understood self-interest, but also with a view to stimulating global development.

Internet Governance As a Task for German Policy-makers

The term "Internet governance" is politically contested. This is no small problem for scholarly analysis, as the subject itself is already controversial.[1] One way of dealing with this challenge is to define the term Internet governance so broadly that it covers all political phenomena somehow related to the Internet.[2] In this study, however, the practice of Internet governance is examined on the basis of a narrower, analytical conception of governance, which at the same time highlights the political significance of this practice.

Governance

The starting point for the understanding of Internet governance proposed here is a definition of governance that Thomas Risse and Tanja Börzel prominently introduced in the political science debate on "governance". They define governance as institutionalised forms of political coordination "to produce and implement collectively binding rules, and/or to provide collective goods".[3] Based on this understanding of governance, Internet governance is defined as the sum of all those institutionalised forms of political coordination aimed at setting binding rules and/or providing collective goods in relation to the Internet.

It is deliberately kept open in this context as to which actors set the rules or provide goods and how they do this. In particular, this is intended to raise awareness of the fact that governance is not always a matter solely for the state. At the same time, the definition draws attention to the fact that it is about the intentional provision of collective goods. Thus, unintended effects cannot be described as governance, and neither does conscious coordination to spread evils qualify as governance (e.g. in the form of organised crime).[4]

Specific governance constellations always reflect the power relations between the actors involved. This explains why governance is always in need of justification. This applies in particular to the setting and enforcement of collectively binding rules, that is, the exercise of authority. But there is also a need for justification in the provision of collective goods if it takes place against the background of existing power asymmetries and if it is likely to perpetuate them.

Tasks and Goals of German Policy-makers

As technical as Internet governance may often seem, at its core it is about fundamental questions of politics. Which institutions and actors have the right to set rules on the basis of which procedures, that is, to exercise authority? Which institutions and actors are responsible for providing which collective goods and under which conditions? Which interests are pursued

1 See Jeanette Hofmann, Christian Katzenbach, and Kirsten Gollatz, "Between Coordination and Regulation. Finding the Governance in Internet Governance, *New Media & Society* 19, no. 9 (2016): pp.. 1406–23; Julia Pohle, Maximilian Hösl and Ronja Kniep, "Analysing Internet Policy As a Field of Struggle", *Internet Policy Review* 5, no. 3 (2016): 1–21.

2 See Laura DeNardis, *Protocol Politics. The Globalization of Internet Governance* (Cambridge, MA, 2009), 14.

3 Tanja Börzel, Thomas Risse and Anke Draude, "Governance in Areas of Limited Statehood. Conceptual Clarifications and Major Contributions of the Handbook", in *The Oxford Handbook of Governance and Limited Statehood*, ed. Tanja Börzel, Thomas Risse and Anke Draude (Oxford: Oxford University Press, 2018), 3–25.

4 Tanja Börzel and Thomas Risse, "Governance without a State. Can It Work?", *Regulation & Governance* 4 (2010): 113–34 (115).

Box 1
Public and collective goods

Public goods are distinguished from private goods by two conditions: (a) access to them is equally free for all (non-excludable), and (b) the use of the goods by one person does not restrict the use for others (non-rival). Both conditions are based on political provisions. Whether, for example, knowledge is treated as a public or private good is by no means determined by the matter itself. Collective goods differ from public goods in that only one of these two conditions must be fulfilled.[a]

a Tanja Börzel, Thomas Risse and Anke Draude, "Governance in Areas of Limited Statehood. Conceptual Clarifications and Major Contributions of the Handbook", in *The Oxford Handbook of Governance and Limited Statehood*, ed. Tanja Börzel, Thomas Risse and Anke Draude (Oxford: Oxford University Press, 2018), 3—25.

in this process, and how does this affect power relations?[5]

Just as the Internet is a global communications network, so too do these issues have global reach — and therefore always also fall within the scope of foreign policy. Traditionally, however, in many countries Internet governance is primarily treated as an economic policy issue. In Germany, too, the Federal Ministry of Economic Affairs (BMWi) is the lead agency within the federal government. In particular, the ministry is responsible for representing Germany at the ITU and ICANN; the BMWi is also responsible for organising the IGF in 2019 (see Box 3, p. 12). The Federal Ministry of Transport and Digital Infrastructure, the Federal Ministry of the Interior, Building and Home Affairs, and the Federal Foreign Office are regularly involved. The way in which the topic is dealt with in the Bundestag corresponds to this division of responsibility on the part of the ministries; however, questions of global Internet governance in particular receive little attention here.

Since there has been no broader debate on the global Internet infrastructure to date, public statements on the goals of German policy in this area have also been limited. Nevertheless, some fundamental objectives can be derived from the general principles of German foreign policy, from the "Digital Agenda" published by the federal government in 2014, and from a number of statements, in particular by the BMWi:

- #Z1: Promoting the digital economy. Across all political camps, in Germany the Internet is perceived as an opportunity for economic development. Although there are repeated reminders of the potential negative consequences of the Internet for parts of the labour market, positive expectations prevail. The buzzword "Industry 4.0", for example, has recently attracted much attention. The "Digital Agenda" of 2014 contains an explicit reference to the regulatory goal of free and fair competition.[6] In the context of the political discussions on global Internet governance, this can be understand as setting the goal of maintaining the Internet as a worldwide communication medium for economic activities and, if possible, expanding it further.
- #Z2: Strengthening the security of IT systems. In Germany, the security of IT systems plays an important role in the digital policy debate. The topic has attracted much attention in recent years as a result of hacker attacks on the Bundestag and the federal government's network. In addition, companies report an increase in economically motivated attacks. The goal of making the use of the Internet secure for public authorities and companies, but also for individual citizens, can be extended to the level of global Internet governance: A sufficient level of security of the global Internet infrastructure is a prerequisite for the security of Internet services that make use of this infrastructure.
- #Z3: Protection of human rights also in the digital space. Human rights are recognised as one of the central normative orientation points of German foreign policy. In recent years in particular, the federal government has repeatedly emphasised that this also applies to digital space. Germany's commitment to the Freedom Online Coalition sends a clear signal in this direction. The main focus is on the right to privacy, freedom of opinion, and freedom of the press.[7] At the end of 2018, the federal government endorsed Tim Berners-Lee's proposal for a "Contract for the Web", which empha-

5 See Laura DeNardis, *The Global War for Internet Governance* (New Haven, CT: Oxford University Press, 2014).

6 Die Bundesregierung, *Digital Agenda 2014–2017* (Berlin, 2014), 4, https://www.bmwi.de/Redaktion/EN/Artikel/Digital-World/digital-agenda.html (accessed 14 March 2019).

7 Auswärtiges Amt, *International Cyber Policy*, https://www.auswaertiges-amt.de/en/aussenpolitik/themen/cyber-aussenpolitik (accessed 14 March 2019).

sises free access to the Internet and the right to privacy.[8] This repeated commitment to the application of human rights in the digital space also leads to objectives for the level of Internet infrastructure. After all, it is here that the technical course is set for whether and to what extent censorship is made possible, or how the privacy of Internet users is protected.

- #Z4: Strengthening multi-stakeholder governance. With particular regard to the context of global Internet governance, the federal government has for many years explicitly committed itself to multi-stakeholder governance. In 2015, for example, the BMWi, together with a number of German interest groups, clearly declared itself in favour of transferring the administration of the DNS (see Box 2, p. 12) to ICANN. One of the main reasons given was that this institution was organised in accordance with the multi-stakeholder model.[9] The Bundestag's Enquete Commission on Internet and Digital Society also clearly positioned itself in favour of this model in a report from 2013. Not least, the federal government is prominently supporting the IGF (see Box 3, p. 12) by hosting the forum in 2019.
- #Z5: Maintaining interoperability. The commitment to the existing structures of multi-stakeholder governance is often closely tied to the goal of interoperability.[10] Essentially, interoperability refers to the possibility that the various elements of the Internet can communicate with each other despite their technical diversity. The Internet consists of numerous subnets, connects the most diverse types of devices, and is used for the most diverse purposes. Data exchange across these various forms of use is not always desirable; in principle, however, it is possible as long as everyone uses the same infrastructure. The technical concept of interoperability can therefore be translated into the political goal of maintaining the globally unified infrastructure of the Internet.

8 Marie-Charlotte Matthes, "Schnelles und offenes Internet für alle: Bundesregierung unterzeichnet 'Contract for the Web'", *netzpolitik.org* (online), 28 November 2018, https://netzpolitik.org/2018/schnelles-und-offenes-internet-fuer-alle-bundesregierung-unterzeichnet-contract-for-the-web/ (accessed 14 March 2019).

9 BMWi, *Position deutscher Interessengruppen. Leitlinien und Handlungsempfehlungen zur Überleitung der Aufsicht über die IANA-Funktionen* (Berlin, 2015).

10 See etwa Deutscher Bundestag, 17. Wahlperiode, Drucksache 17/12480, *Elfter Zwischenbericht der Enquete-Kommission "Internet und digitale Gesellschaft". Internationales und Internet Governance* (28 February 2013), 20.

The Current Model of Internet Governance

The origins of the Internet have their roots in substantial public investments. A key driver was the US military's interest in a decentralised communications system. At the beginning of the 1990s, however, the Clinton administration opted for a far-reaching policy of privatisation: The task of further developing the Internet and creating a corresponding infrastructure for the general population was entrusted to private companies.[11]

In the course of the global spread of the Internet, this model was adopted by most countries. Access to the Internet is usually provided by private Internet service providers (ISPs), which either connect directly to global network operators or use privately operated Internet nodes (Internet exchange points, IXPs) to connect to the global network. The latter, in turn, consists of a complex of fibre-optic and satellite connections, most of which are also privately owned.

This prominent role of private actors is also reflected in today's Internet governance structures. ISPs, IXPs, and providers of Internet services are subject to the legal requirements of the countries in which they offer their services. Those technical standards, however, which create the global and domestic basis for communication on the Internet, are developed by private actors. Non-hierarchical cooperation comprises the dominant form of governance here (see p. 7), with the addition of ICANN's limited claim to authority (see Table 1).

The distinction between *Internet services* and *Internet infrastructure* is analytically helpful. Since the 1990s, a large number of Internet services have emerged, ranging from simple websites and chat rooms to today's social networks and messaging services.

11 Ev Ehrlich, "Thanks to Bill Clinton, We Don't Regulate the Internet Like a Public Utility", *Forbes* (online), 17 May 2014, https://www.forbes.com/sites/realspin/2014/03/17/thanks-to-bill-clinton-we-dont-regulate-the-internet-like-a-public-utility/ (accessed 19 December 2018).

The Internet's mode of operation relies on the premise that all of these different services are ultimately based on a manageable set of basic protocols for transmitting data. These protocols are referred to as the logical infrastructure of the Internet (whereby "logical" here is essentially to be understood as a reference to software). They are designed to enable the various forms of Internet usage to be brought together in a unified technical structure. This structure follows a layered architecture; the higher layers contain more specific protocols and are based on the lower layers. It is common today to describe the logical infrastructure as a whole using the Transmission Control Protocol/ Internet Protocol (TCP/IP) model. In addition, there is the physical infrastructure in the form of cable connections, routers, and servers.

Global Standards

The logical infrastructure of the Internet therefore consists of a series of standards and protocols. Prominent examples are Hypertext Markup Language (HTML) for displaying websites and the Unicode standard for merging different font and character systems. For the most part, such standards and protocols are developed and made available by private actors. These come together in institutions such as the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), and the World Wide Web Consortium (W3C). In principle, participation is open to all interested parties. In fact, however, the technical level required for such participation is so high that it is mainly representatives of key companies and, to a limited extent, scientists who gather here. The Internet Architecture Board (IAB) provides an impression of the usual composition of such institutions. Within the IETF, it exercises a limited supervisory function over standard-setting processes. Of the twelve members of this committee, ten are currently

Table 1

The field of global Internet governance

	Authoritative rule-setting	**Provision of public/ collective goods**
Internet services	States: laws and regulations	Civil society: e.g. creative commons, open source
Internet infrastructure		
logical (TCP/IP)		
application layer (e.g. HTTP, FTP, DNS)	ICANN: DNS	IETF, W3C: Standards
transport layer (e.g. TCP, UDP)	—	IETF: Standards
network layer (e.g. IP)	—	IETF: Standards
network access layer (e.g. Ethernet)	—	IEEE, ITU: Standards
physical		
cable, router, server (IXPs, ISPs)	States: laws and regulations	IETF, IEEE: Standards

working for companies in the Internet industry, while two are scientists from universities.[12]

The standards and protocols developed in forums such as the IETF, the IEEE, and the W3C are public goods (see Box 1, p. 8). They are made publicly available and are free to use by everyone (non-excludable), and they can be used by an unlimited number of people (non-rival). In fact, it is actually in the interest of those who develop these protocols that they be used as much as possible.[13]

The standards are developed on the basis of voluntary cooperation. The dissemination of the standards is also voluntary in form. An institution such as the IETF cannot dictate to states or companies which standards they have to use. In this sense, this is a case of the non-hierarchical provision of a public good (see Table 1).

The absence of formal hierarchies, however, does not mean that power relations do not exist. In particular, the companies concerned try to assert their interests in the committees of institutions such as the IETF. A current example of this is the strong involvement of the Chinese company Huawei in shaping the new 5G mobile communications standard.[14] Companies also use their market power to help certain standards achieve widespread adoption.

Authoritative Rule-setting by ICANN

The Internet Corporation for Assigned Names and Numbers occupies a special position in the structure of global Internet governance. For one thing, it authoritatively sets collectively binding rules for the DNS (see Box 2). ICANN thus determines how, and under what conditions, domain names and IP addresses are allocated on the Internet. Second, the organisation provides a central public good for the Internet's global infrastructure by managing the DNS root zone, the central database in the Internet's address system.[15]

12 *Internet Architecture Board – Members*, https://www.iab.org/about/iab-members/ (accessed 18 April 2019).

13 Joseph S. Nye, *The Regime Complex for Managing Global Cyber Activities* (Waterloo: Global Commission on Internet Governance, 2014), 6, https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf (accessed 14 September 2018).

14 Raymond Zhong, "China's Huawei Is at Center of Fight Over 5G's Future", *The New York Times* (online), 7 March 2018, https://www.nytimes.com/2018/03/07/technology/china-huawei-5g-standards.html (accessed 6 February 2019). See also Daniel Voelsen, Tim Rühlig, and John Seaman, *5G and the US–China Tech Rivalry – a Test for Europe's Future in the Digital Age. How Can Europe Shift from Back Foot to Front Foot?*, SWP Comment 29/2019 (Berlin: Stiftung Wissenschaft und Politik, June 2019).

15 See https://pti.icann.org and https://www.iana.org.

Box 2
The Domain Name System (DNS)

As a global communications network, the Internet operates on the principle that all devices connected to it can exchange information with each other. This requires all devices to have individual addresses. Each device is assigned a numerical IP address (at least temporarily) for this purpose. The common format for such IP addresses is IPv4 (e.g. 192.0.43.7). The new IPv6 standard (e.g. 2606:2800:220:1:248:1893:25c8:1946) offers a much larger address space and has, for some years, been introduced in parallel to the previous IPv4 standard. Domain names (e.g. www.example.com) that refer to these IP addresses are intended to make it easier for human users to exchange information on the Internet.

In this sense, the global address directory of the Internet links domain names and IP addresses. It consists of a large number of databases, each of which covers specific address ranges. Many ISPs also keep copies of the most important data for their customers in their own networks. As a whole, this network of databases is called the Domain Name Systems, or short: DNS. Contrary to the widespread rhetoric of the Internet as a decentralised network, the DNS is organised strictly hierarchically. The various partial databases for individual address ranges (such as the .de domain) are linked together via a central database, the so-called DNS root zone.

Box 3
The Internet Governance Forum (IGF)

The United Nations prominently took up the idea of multi-stakeholder governance by founding the IGF, which was launched at the World Summit on the Information Society (WSIS) in 2005; since then, the UN General Assembly has extended its mandate twice. At its core, the IGF consists of an annual conference bringing together various stakeholders from all over the world. It explicitly has no mandate to make binding decisions. Rather, the forum's discussions are meant to form the basis for voluntary cooperation, and for binding decisions in other institutions.

After initial enthusiasm, today the IGF finds itself in a difficult situation. Its unique feature — the link to the procedures of the UN system — is increasingly perceived as a limitation. The Internet Governance Project (IGP), which was founded by Milton Mueller and others, for instance, criticises the great influence that the states are thereby securing for themselves. In addition, members of the IGP fear that increasingly only member states from the OECD will be able to host the forum because the UN places such high demands on the respective host.[a]

Against this background, the difficulty in finding a host country for the IGF 2018 was symptomatic. Only a few months before the planned date, France showed itself ready to host the meeting. The UNESCO premises could be used to meet the requirements for UN conferences. President Emmanuel Macron combined the event with two other long-planned international digital conferences of the French government — thus emphasising his demand for a stronger link between the IGF and multilateral decision-making processes.[b] In 2019, Germany will host the IGF.

a International Governance Project (IGP), *International Internet Policy Priorities. IGP Advises the NTIA* (Atlanta, GA, 2018), 1—14 (12ff.), https://www.ntia.doc.gov/files/ntia/publications/igp-comments.pdf (accessed 3 July 2018). See also Milton Mueller, *The Paris IGF: Convergence on Norms, or Grand Illusion?* (International Governance Project, 9 November 2018), https://www.internetgovernance.org/2018/11/09/the-paris-igf-convergence-on-norms-or-grand-illusion/ (accessed 14 November 2018).

b Internet Governance Forum, "IGF 2018 Speech by French President Emmanuel Macron", 13 November 2018, https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron (accessed 13 December 2018).

Legitimacy through Multi-stakeholder Governance

Like any institutional order, today's system of global Internet governance is in need of justification. The technical expertise of institutions such as ICANN and the IETF is repeatedly referred to as a legitimising factor, as is the voluntary nature of the standards and protocols developed.[16]

In addition, with a view to the specifically political dimension of Internet governance, the idea of multi-stakeholder governance has found widespread acceptance. The basic idea is to include all those who have a stake in the further development of the Internet. In practice, this usually includes companies, states, academia, and various civil society actors. For example, the IETF and the W3C are characterised by the open and largely informal involvement of companies, independent experts, and scien-

16 See Monika Ermert, "Missing Link. Der Angriff auf das offene Internet und die Ethik des Netzes", *heise online*, 5 August 2018, https://www.heise.de/newsticker/meldung/Missing-Link-Der-Angriff-auf-das-offene-Internet-und-die-Ethik-des-Netzes-4129289.html (accessed 4 September 2018).

tists. ICANN also has a number of advisory bodies that are involved, via formalised procedures, in the decisions of the ICANN Board.

Conflicts over the Global Infrastructure of the Internet

With the existing Internet governance structures, the possibilities for using the Internet have expanded massively. One of the most important changes has been the turn to mobile devices as access points to the Internet. In addition, there are now many forms of interactive use of Internet services, not only in social media, often referred to as "Web 2.0". Another important trend is the growing importance of the "cloud". Data storage and processing are shifting away from individual devices to large data centres. The mobile Internet and the "cloud", together, form the basis for the technological development that is expected to shape daily life in the coming years: the connection of ever more devices in business, administration, and private households into what has been dubbed the "Internet of Things".

However, it is also evident that the current model of Internet governance systemically reaches its limits where genuinely political conflicts arise. Explanations for this can be found in recent political science research on non-state governance:

- #E1: First, the potential of non-governmental governance is limited by the mere number of actors involved. Voluntary coordination requires a minimum level of trust, as there is no authority that can officially sanction misconduct. In small social groups, personal contacts create trust; at the same time, there are ways to punish undesirable behaviour through various forms of social ostracism.[17] If one looks at the history of Internet governance, it becomes apparent that, initially, it was in fact strongly influenced by personal relationships. In the familiar talk of the "fathers of the Internet", a correspondingly personalised understanding of governance comes to the fore — as well as the reluctance to acknowledge the contribution of women such as Sharla Boehm and Elizabeth "Jake" Feinler to the development of the Internet.[18] With the global expansion of the Internet, however, the number of actors involved has increased significantly. Even though it is difficult to measure this empirically, it can be assumed that trust based on personal relationships has diminished accordingly.
- #E2: A second systematic problem of non-hierarchical governance arises if there is no agreement on the services to be provided. In such cases, the willingness to cooperate voluntarily decreases, and it quickly turns out that non-governmental forms of governance usually do not have the necessary legitimacy to decide on such matters.[19] In the specific context of Internet governance, the main problem is that a growing number of states see the Internet as a means of asserting their respective interests — and thus come into conflict with each other and with non-state actors in Internet governance.
- #E3: Closely related to this is a third problem of non-state governance, namely that it is determined — not surprisingly — by the interests of private actors. In the case of Internet governance, these are mainly companies whose primary organisational purpose is to increase their own profits. Such non-governmental governance is therefore unsuitable for problems whose solution does not generate profit, or even generates costs. One example is the persistently low proliferation of IPv6 addresses (see Box 2, p. 12). These addresses offer a solution to the problem that the number of addresses available under the current IPv4 standard is limited and

17 Anke Draude, Lasse Hölck and Dietlind Stolle, "Social Trust", in *The Oxford Handbook of Governance*, ed. Börzel et al. (see note 3), pp. 353–72.

18 On the issue of the "Mothers of the Internet", see the answers to the following tweet: https://twitter.com/d_voelsen/status/1098898783004446726.

19 Daniel Jacob, Bernd Ladwig and Cord Schmelzle, "Normative Political Theory", in *The Oxford Handbook of Governance*, ed. Börzel et al. (see note 3), 564–83.

will not be sufficient in the long term to connect all devices directly to the Internet. The switch to IPv6 is not politically controversial, but it conflicts with the economic interests of network operators. So far, they have often been unwilling to bear the costs of the migration — not least because they cannot pass them on to their customers.[20]

Security and Privacy in the Domain Name System (DNS)

The DNS is an essential element of the logical infrastructure of the Internet (see Box 2, p. 12). In its current form, however, this system has considerable weaknesses. From a security perspective, the most pressing problem is DNS poisoning. With this method, DNS information in a sub-network is manipulated in such a way that a user request for a domain refers to a different IP address than the one actually registered for that domain. Calling the domain example.com would then lead to a page that looks like the original page to the user, but that is actually a copy which serves to load malware onto the user's computer or to extract critical data such as passwords.

An attempt to counter this problem, which is now quite widely used, consists in issuing encrypted certificates (see Box 4). These cannot in themselves prevent "DNS poisoning", but they do offer some protection against such attacks. If a request to example.com is redirected to another IP address, the visited server cannot send the SSL certificate belonging to example.com — and a corresponding warning appears in the browser. The problem, however, is that the SSL certificate systems in existence today have their own security gaps and are still only used on 70 to 80 per cent of all websites.[21] In addition, many websites use outdated or incorrectly configured variants of the SSL protocol.[22] Moreover, it is possible to embed legitimate SSL certificates on "fake" websites. With sufficient effort, an Internet user can thus be redirected to a page that not only looks like the original page, but also offers supposedly secure SSL encryption.[23]

The so-called Domain Name System Security Extensions (DNSSEC) are intended to provide a direct remedy against "DNS poisoning". They are used to digitally sign DNS data. This is to ensure that DNS data originates from trustworthy sources. However, DNSSEC is considered complicated and therefore prone to errors.[24]

In its present form, the DNS also offers far-reaching opportunities to invade the privacy of Internet users. To date, all DNS queries have been unencrypted; even DNSSEC does not encrypt DNS queries. Thus, it is quite simple to determine which domains an Internet user requests from the DNS. Many countries take advantage of this to specifically block certain domains.

This problem too has been known in the technical community for some time. There are, for example, advanced proposals to combine DNSSEC with encryption mechanisms (see Box 4, p. 15). The basic idea here is to route DNS queries via encrypted connections (e.g. "DNS over TLS", "DNS over HTTPS"). In this way, requests would only be processed by certified bodies using encrypted channels. Such a combination of certification and encryption would make "DNS

Box 4
Encryption (TLS, SSL, HTTPS)

Various types of data are encrypted for transmission over the Internet using the Transport Layer Security (TLS) protocol. This protocol is the successor of the long-used Secure Socket Layer (SSL) protocol. The use of TLS in the representation of websites is well-known; here, the Hypertext Transfer Protocol (HTTP) protocol is supplemented by an encryption component (HTTPS). If a web server provides such encryption, this can be easily recognised by the address of the website. If a web server offers this type of encryption, it can be identified by the address of the web site. The address starts with "https" instead of "http" (e.g. https://www.swp-berlin.org). In addition, many modern browsers now indicate when a website is not encrypted using https. TLS can also be used for other purposes, such as encrypting access to e-mail servers.

20 Brenden Kuerbis, "IPv6 Deployment around the World. A New Digital Divide?", *CircleID*, 25 January 2018, http://www.circleid.com/posts/20180125_ipv6_deployment_around_the_world_a_new_digital_divide/ (accessed 23 August 2018).

21 Let's Encrypt, *Let's Encrypt Stats*, 2018, https://letsencrypt.org/stats/ (accessed 13 December 2018).

22 Monika Ermert, "TLS 1.2. Client-Zertifikate als Tracking-Falle", *heise online*, 20 July 2018, https://www.heise.de/security/meldung/TLS-1-2-Client-Zertifikate-als-Tracking-Falle-4117357.html (accessed 14 March 2019).

23 See Andy Greenberg, "Cyberspies Hijacked the Internet Domains of Entire Countries", *Wired*, https://www.wired.com/story/sea-turtle-dns-hijacking/ (accessed 2 May 2019).

24 IANIX, *DNSSEC Downtime: List of Outages & Validation Failures*, 2018, https://ianix.com/pub/dnssec-outages.html (accessed 13 December 2018).

poisoning" considerably harder, protect the privacy of Internet users more strongly, and make government censorship more difficult.[25]

Law enforcement and security agencies often want to use existing weaknesses in the DNS for their purposes.

The problem of security and data protection in the DNS is thus well-known, and solutions have already been proposed. However, it has not been possible to implement them comprehensively at the level of the global infrastructure. This can be explained by the limitations of non-governmental governance mentioned in the previous section.

Firstly, from a historical perspective, the security problem of DNS poisoning is a consequence of the massive expansion of the Internet. In its founding phase, there were only a limited number of institutions processing DNS queries. These institutions could be trusted largely without recourse to complex certification mechanisms (#E1). This type of trust-based communication, however, is no longer feasible today.[26]

Secondly, measures to improve security and data protection in the DNS are politically controversial (#E2). In principle, all states have an interest in a secure global Internet infrastructure. At the same time, however, the law enforcement and security agencies in many countries want to use the existing security gaps in the DNS for law enforcement purposes or to restrict access to certain content. In liberal-democratic states, too, DNS-based filters are used to impede access to child pornography.

Thirdly, both the certification and the encryption of DNS queries generate additional costs for network operators. In addition to the direct costs for the introduction of appropriate technical precautions, network operators fear indirect costs, which are incurred because common methods of data traffic management are no longer possible with encrypted DNS requests. Since few consumers and businesses are aware of the security risks in the DNS, it is difficult for network operators to pass these costs on to their customers (#E3).

Mozilla's efforts to encrypt DNS queries at the browser level provide a counterpoint to this. The aim here is to position the Firefox browser as an alternative for privacy-focussed Internet users. For the initial test phase, Mozilla chose the US-based company Cloudflare to resolve the cryptographically secured DNS requests. The fact that, with this system, a single company collects all DNS queries has caused a lot of criticism. As a reaction, Mozilla announced its intention to cooperate with other DNS resolvers in the future.[27] Google also offers DNS request encryption and, by default, directs all DNS queries in its Chrome to its own DNS service (accessible via IPv4 at 8.8.8.8). However, Google's motivation is not to enhance their users' privacy; as the company clearly states, it uses the data to obtain information to improve its own services, and possibly also for advertising purposes.[28]

The activities of Mozilla and Google point to a structural problem of today's Internet governance. In some respects, it has become virtually impossible to upgrade the global Internet infrastructure. This invites powerful players to develop their own solutions. In the case of the DNS, there is no less at stake than the future of a globally uniform address system.

Security in the Routing System

The Internet was originally designed to allow all connected devices to communicate directly with each other. The decentralised logic of the Internet therefore still requires that the most important tasks in the transmission of data are performed by the end points, whether these are end-user devices, servers, or sub-networks.

One consequence is that there are neither technical nor legal requirements specifying along which waypoints a data ("packets") is routed through the global Internet. Various organisations such as large companies, government units, and above all ISPs operate sub-networks of the Internet, so-called autonomous

25 Open Rights Group, *DNS Security – Getting It Right*, 2019, https://www.openrightsgroup.org/about/reports/dns-security-getting-it-right (accessed 4 September 2019).

26 Edward Lewis, "DNS. A Look Back at a Look Back", *Blog*, 19 August 2018, https://blog.apnic.net/2018/08/09/dns-a-look-back-at-a-look-back/ (accessed 23 August 2018).

27 Monika Ermert, "DNS over HTTPS und die Privatsphäre der Nutzer: Mozilla will nicht nur einen Resolver", *heise online*, 28 March 2019, https://www.heise.de/newsticker/meldung/Mozilla-zu-DoH-Resolvern-Es-soll-nicht-nur-einen-geben-4354060.html (accessed 18 April 2019).

28 See https://developers.google.com/speed/public-dns/privacy and https://policies.google.com/privacy?hl=en#whycollect.

systems. As operators of these sub-networks, they inform other operators which connections they can offer at which speeds. The basis for this is the Border Gateway Protocol (BGP). A German ISP would thus signal, for example, that it can offer particularly fast connections to end points in Germany and France. As all operators of sub-networks make such information public, a kind of map is created that shows which connections are fastest at a given point in time.

The crucial point now is that this exchange has so far been based entirely on trust (#E1). The information provided by sub-network operators is not systematically verified. Thus, it is possible that individual operators publish false information, and thus change the global data traffic. The reason can simply be a configuration error. However, recently there has been an increase in incidents that are suspected of being politically motivated. The logic behind this is simple: If a state directs data traffic through its territory or autonomous systems under its control, it thereby gains the opportunity to analyse or filter the traffic. This procedure is called BGP hijacking.[29] The following examples illustrate the problem:

- In April 2010, for 18 minutes China Telecom routed about 15 per cent of global Internet traffic through Chinese servers. This also affected data traffic involving domains belonging to the US government (.gov) and the US military (.mil).[30] A report published at the end of 2018 points out that, since 2016, China Telecom has been routing data traffic from the United States via BGP hijacking through Chinese servers in a number of other cases. The company's "points of presence" in the United States and Canada were used for this purpose.[31]
- As the revelations of whistleblower Edward Snowden show, the National Security Agency (NSA) has also relied on BGP hijacking to redirect traffic in the past, though it seems to have preferred the euphemistic term "traffic shaping". The NSA's documents describe in detail the corresponding technical procedure, using Yemen as an example.
- On 30 July 2018, the Telecommunication Company of Iran redirected the traffic to the servers of the widely used messaging service Telegram for a period of about one hour. The immediate effect was that Telegram was no longer usable as a messaging service at that time.[32] Already at the beginning of 2018, the government in Tehran had tried by various means to technically prevent the use of Telegram within the country.

Even though cases like these seem to be accumulating lately, the problem has been known for many years.[33] Again, there is no lack of technical solutions. Just as DNSSEC supplements the DNS with certification mechanisms, there is a proposal to secure the BGP protocol with certification mechanisms (Border Gateway Protocol Security, BGPSec).[34] One idea here is that the operators of autonomous systems secure their routing information with a certificate and themselves only use information that is certified. In this way, the source of the routing information could be identified at any time, even in a decentralised system, and the reliability of the source could be assessed. In addition, the Internet Society, an influential non-governmental organisation in the field of Internet governance, has drawn up a catalogue of practical measures to secure the routing system — the Mutually Agreed Norms for Routing Security (MANRS). To date, however, they have only been supported by a few companies.[35]

29 It should be noted, though, that there are also cases of BGP hijacking that have primarily financial motives; see Doug Madory, "BGP/DNS Hijacks Target Payment Systems", *Oracle*, 3 August 2018, https://blogs.oracle.com/internetintelligence/bgp-dns-hijacks-target-payment-systems (accessed 7 August 2018).

30 Nate Anderson, "How China Swallowed 15% of 'Net Traffic for 18 Minutes", *Ars Technica*, 17 November 2010, https://arstechnica.com/security/news/2010/11/how-china-swallowed-15-of-net-traffic-for-18-minutes.ars (accessed 9 July 2018).

31 Chris Demchak and Yuval Shavitt, "China's Maxim — Leave No Access Point Unexploited. The Hidden Story of China Telecom's BGP Hijacking", *Military Cyber Affairs* 3, no. 1 (2018): 1—9.

32 "Iran's Telecommunications Company Illegally Rerouted Telegram App Traffic", *GlobalVoices advox*, 6 August 2018, https://advox.globalvoices.org/2018/08/06/irans-telecommunications-company-illegally-rerouted-telegram-app-traffic/ (accessed 15 August 2018).

33 See Kim Zetter, "Revealed: The Internet's Biggest Security Hole", *WIRED*, 26 August 2008, https://www.wired.com/2008/08/revealed-the-in/ (accessed 14 November 2018).

34 See M. Lepinski and K. Sriram, *RFC 8205: BGPsec Protocol Specification*, September 2017, https://tools.ietf.org/html/rfc8205; Geoff Huston, "Securing the Routing System at NANOG 74", *CircleID*, 16 October 2018, http://www.circleid.com/posts/20181016_securing_the_routing_system_at_nanog_74/ (accessed 17 October 2018).

35 *Mutually Agreed Norms for Routing Security*, https://www.manrs.org/ (accessed 19 December 2018).

These proposals are politically controversial (#E2). As described above, the intelligence services of some states have a proven interest in not fixing security vulnerabilities. A further complicating factor is that it would be very costly for the operators of the autonomous systems to make changes to the existing system (#E3). They would have to update their own infrastructure, and then fear the associated transparency. If an operator were obliged to make verifiably accurate data about its connection capacities public, it would be deprived of a means of controlling data traffic that passes through its network.[36]

Here, too, the limits of non-hierarchical governance reveal themselves. It is remarkable that even the Internet Society — otherwise better known as a critic of state activity in Internet governance — explicitly addresses "policy-makers" when it comes to routing security and calls on them to act: "Through leading by example in their own networks, strengthening communication, and helping realign incentives to favour stronger security, policy-makers can help improve the routing security ecosystem."[37]

As with the DNS, the unsolved issues with the Internet's routing system raise the threat of fragmentation. According to the report on China Telecom mentioned earlier, BGP hijacking by the company was essentially made possible by the fact that it has had several "points of presence" in the United States since the early 2000s. Such a local presence makes it easier to redirect data traffic in the United States or traffic passing through the United States. Conversely, there are no non-Chinese "points of presence" in China. The authors of the report argue for more reciprocity here. However, China's approach also points to the opposite possibility, namely national isolation. If the problems of routing security cannot be solved globally, it is feared that other states will choose this path in the future.

Security and Availability of Submarine Cables

The talk of the Internet as a "logical space", the metaphor of data clouds ("clouds"), and, last but not least, the enormous technical advances in the field of wireless data transmission with WLAN, Bluetooth, and mobile networks — all of these almost make one forget that the Internet is dependent on a tangible physical infrastructure. Submarine cables occupy a prominent position in this context. Mainland cable connections and mobile radio networks are territorially limited, whether to individual regions, states, or, in the case of Europe, the respective continent. Only a very small part of the connection between these areas uses satellite links, whereas the rest is mainly routed via submarine cables.

It is noteworthy that around 95 per cent of the world's submarine cable network is owned by private companies.[38] Usually the operators provide the transmission capacities of the cables for a fee. In addition, there are contractual agreements under which large operators make certain data transmission capacities available to each other.[39] The provision of data transfer capacity is thus clearly a private — and not a collective — good (see Box 1, p. 8). Also, there is no global institution that claims the right to set collectively binding political rules in this area. Institutions such as the IETF and the W3C focus exclusively on the development software protocols, whereas institutions such as the IEEE and the ITU only address some of the technical challenges of cable systems.[40]

"Chokepoints" As a Security Threat

Little attention is thus paid to the specific security threats that this part of the Internet infrastructure is exposed to. The existing network of submarine cables has a high concentration of routes and landing sites; these "chokepoints" create considerable vulnerability.[41] Examples are the Suez Canal, through which

36 See Russ White, "BGP Hijacks: Two More Papers Consider the Problem", *CircleID*, 6 November 2018, http://www.circleid.com/posts/20181106_bgp_hijacks_two_more_papers_consider_the_problem/ (accessed 14 March 2019).

37 Internet Society, *Routing Security for Policymakers: An Internet Society White Paper* (Reston, VA, 2018), https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/ (accessed 14 November 2018).

38 Douglas R. Burnett, Robert Beckman and Tara M. Davenport, eds., *Submarine Cables. The Handbook of Law and Policy* (Leiden, 2013), 9.

39 Mick Green, "The Submarine Cable Industry. How Does It Work?", in *Submarine Cables*, ed. Burnett et al. (see note 38), 42–60 (48).

40 *Submarine Cables*, ed. Burnett et al. (see note 38), 10.

41 Nicole Starosielski, "Strangling the Internet", *Limn*, no. 10 (2018), https://limn.it/articles/strangling-the-internet/ (accessed 14 March 2019).

almost all data connections between Europe and Asia pass, and the landing site in Brazilian Fortaleza, which is used by most of the connections between North and South America (see Fig. 1, p. 20).

This concentration is primarily due to economic considerations (#E3). If an operator has already developed and negotiated routes to a particular landing point, it is much cheaper to use the same route and landing point for new cables than to develop new routes.

These neuralgic points face threats from different angles. Most damage to cables is caused very undramatically by the high strains to which they are exposed under water, such as currents or sharp-edged debris on the seabed. In coastal areas in particular, the cables are repeatedly endangered by fishing boats with trawl nets. In contrast, based on publicly available information, targeted military measures to cut submarine cables are so far only a potential threat. In the past, the fact that Russian submarines were sighted in the vicinity of such cables gave rise to corresponding speculations; in fact, no case has yet become public in which a state has resorted to such means.[42]

Already in 2010 the report "Reliability of Global Undersea Cable Communications Infrastructure" (the ROGUCCI Report) named these risks. The report rightly pointed out that although serious submarine cable disruptions are unlikely, they could have potentially catastrophic consequences if they were to occur: "The impact of such a failure on international security and economic stability could be devastating. It is unclear if civilisation can recover to its previous condition from the failure of a technology that has been so rapidly adopted without a back-up plan."[43]

Whether civilisation as such would be threatened by submarine cable disruptions may be doubtful. However, it is not difficult to imagine the enormous economic damage that would result if, for example, the links between the EU and the United States were to be severed in their entirety. The financial sector and the whole field of international logistics today depends on large amounts of data being transmitted almost in real time worldwide. Even temporary disruptions can thus have considerable consequences. Large-scale interruptions of submarine cables could probably be provisionally compensated by rerouting or recourse to satellite connections. But even then the immediate economic consequences would be considerable. If the importance of these global connections continues to grow in the future, so will their vulnerabilities.

A recent case shows the practical relevance of these considerations. The island of Tonga in the South Pacific is only connected to the Internet via a single submarine cable. For reasons yet unknown, this cable was massively damaged in January 2019. For about two weeks, the island and its population were only connected to the Internet via a satellite connection. The limited data volume provided by this link was used for essential services, for example to enable banks to continue their operations.[44]

Market incentives for cable operators are in tension with the economic needs of developing countries.

As described, there is a low probability that large parts of the network of submarine cables will fail. This explains why most countries see little need for action. If at all, they focus on their immediate environment. In recent years, for example, the United States has increased the requirements for securing landing sites. In 2018 Australia actively prevented the Chinese company Huawei from being commissioned to lay a submarine cable linking the Solomon Islands with the continent.[45] However, the global political dimension of this issue has, so far, been mostly neglected.

The structure of the underlying conflict between states and companies is similar to the disputes about the logical infrastructure of the Internet. Even though many governments have not yet recognised the importance of this issue, it is in the interest of all states that the submarine cable network be protected from

42 Louis Matsakis, "What Would Really Happen If Russia Attacked Undersea Internet Cables", *WIRED*, 1 May 2018, https://www.wired.com/story/russia-undersea-internet-cables/ (accessed 14 March 2019).

43 Karl Frederick Rauscher, *Reliability of Global Undersea Cable Communications Infrastructure*, ROGUCCI report (IEEE Communications Society, 2010), 33, http://www.ieee-rogucci.org/files/The%20ROGUCCI%20Report.pdf (accessed 14 March 2019).

44 "Tonga Hit by Near-Total Internet Blackout", *BBC* (online), 23 January 2019, https://www.bbc.com/news/world-asia-46968752 (accessed 14 March 2019).

45 "Australia Keeps China Out of Internet Cabling for Pacific Neighbor", *Reuters*, 13 June 2018, https://www.reuters.com/article/us-australia-solomonislands-internet/australia-keeps-china-out-of-internet-cabling-for-pacific-neighbor-idUSKBN1J90JY (accessed 20 June 2018).

Figure 1

Larger, more detailed version of this map: http://bit.ly/SWP19RP14SubmarineCables

Concentration of landing points in the worldwide network of submarine cables

The map shows cables that are currently in operation or are expected to be operational by 2022.
It highlights locations where a large number come ashore.

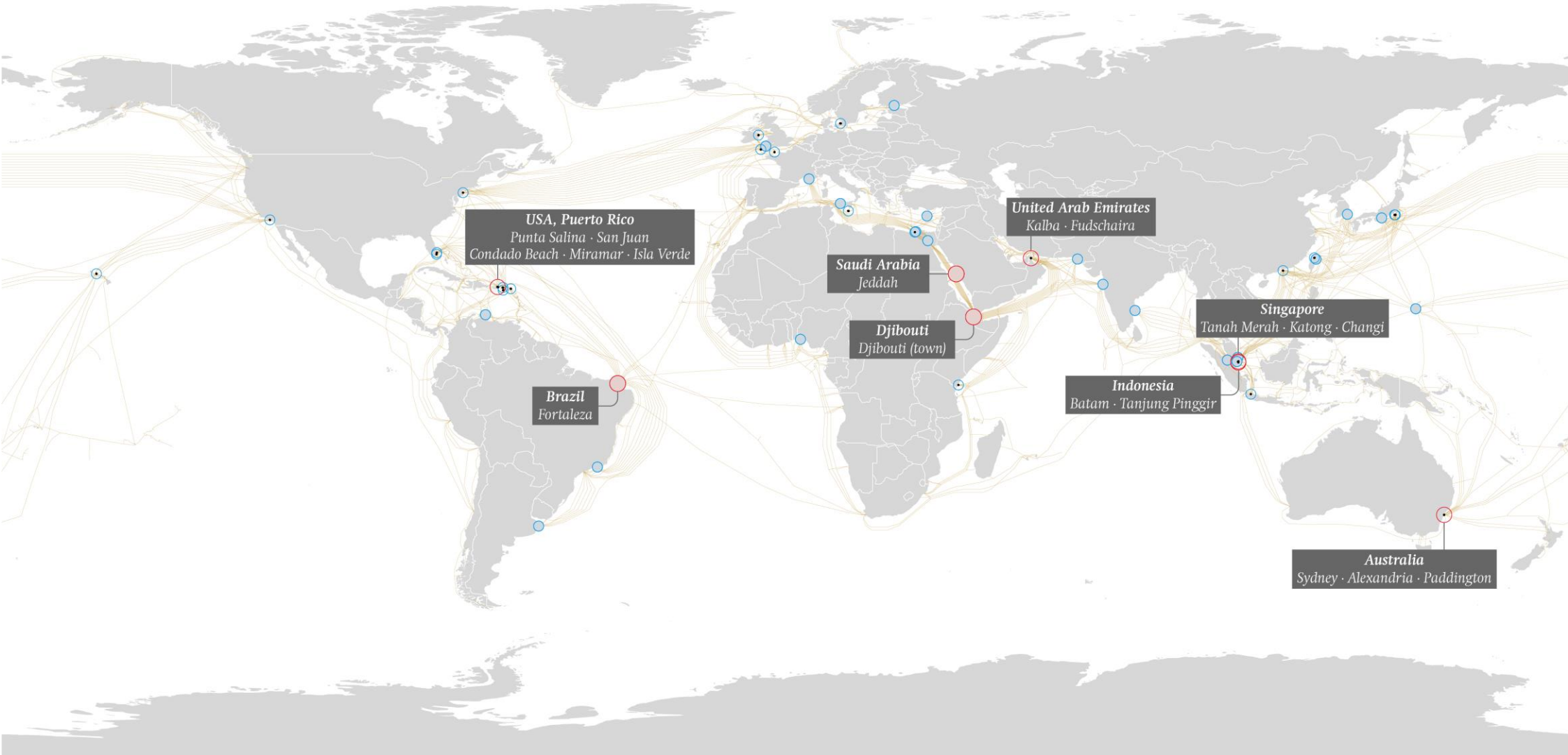
Category 10
Locations where more than 10 cables come ashore at the same landing point *or* locations where more than 10 cables come ashore at a cluster of several landing points in close proximity (no more than 10 kilometres apart from the next landing point).

K10 Landing point **K10** Cluster

Category 5
Locations where more than 5 cables come ashore at the same landing point *or* locations where more than 5 cables come ashore at a cluster of several landing points in close proximity (no more than 10 kilometres apart from the next landing point).

K5 Landing point **K5** Cluster

Source: TeleGeography, www.submarinecablemap.com



widespread failures. This would above all require the creation of redundant structures for the cable connections and landing sites, as well as diversity in the cable and network technology used. However, such measures entail considerable costs. It is not surprising that private submarine cable operators are trying to avoid this financial expense (#E3).

The structure of the underlying conflict between states and companies is similar to the disputes about the logical infrastructure of the Internet. Even though many governments have not yet recognised the importance of this issue, it is in the interest of all states that the submarine cable network be protected from widespread failures. This would above all require the creation of redundant structures for the cable connections and landing sites, as well as diversity in the cable and network technology used. However, such measures entail considerable costs. It is not surprising that private submarine cable operators are trying to avoid this financial expense (#E3).

The Significance for Development Policy

Beyond security issues, the conflict between states and companies over the network of submarine cables reveals itself in debates about the access of developing countries to that network. This access is a very important factor when it comes to harnessing the economic potential of digitalisation. Today, the submarine cable network primarily reflects the current state of global economic relations, as cable operators are primarily guided by economic considerations. A connection between the United States and Europe simply seems more lucrative than one between the United States and Africa.

Cable connections are complex projects and therefore designed for the long term. Economically, the results are lasting path dependencies and even self-fulfilling prophecies. After all, the question of how reliably and at what cost a country is connected to the global Internet infrastructure is likely to have an impact on its economic development. Here, the market incentives for the operators of submarine cables (#E3) are in tension with the economic needs of developing countries.

Authoritative Rule-setting As a Way Out?

So far, there has been little traditional political authority to be found in the institutional structures of global Internet governance. The predominant mode of social coordination here is the non-hierarchical provision of collective goods. When analysing the limits of this institutional arrangement, however, the question arises as to whether more global authority is needed to resolve the conflicts mentioned.

This question gains practical urgency in the conflicts between two central institutions of Internet governance, namely the Internet Corporation for Assigned Names and Numbers and the International Telecommunication Union.

ICANN: Politicisation

ICANN occupies a central position in global Internet governance because the organisation is responsible for the authoritative management of the DNS (see p. 12). In principle, this function would allow ICANN to resolve some of the conflicts surrounding the evolution of the Internet infrastructure through binding rules. For example, ICANN could make the allocation of domains conditional upon the use of security measures such as DNSSEC. Already today, the organisation requires registries of new generic top-level domains (gTLDs) to use DNSSEC in their infrastructure. However, this requirement only affects the registries themselves and not the registrars, the operators of individual domains, or local ISPs.[46]

However, it seems highly unlikely that ICANN's authority will be extended any further, even if this is possible in principle. On the contrary, the organisation is becoming increasingly politicised — even in areas that have so far been largely undisputed.

ICANN and the Role of the United States

The background to this is the special relationship between ICANN and the American government as it exists to this day. For the United States, the global expansion of the Internet has always been linked to the political project of promoting its own liberal ideas of political order.[47] The fact that the American government initially controlled the DNS directly suggests that it has always been aware of the importance of the Internet infrastructure.

Originally, the DNS root zone was administered by the Internet Assigned Numbers Authority (IANA), which in turn was under the control of the US Department of Commerce. In a process lasting several years, however, IANA was transferred to ICANN and finally placed under the control of ICANN's Board of Directors in 2016. The "IANA transition" is regarded as a concession by the United States. However, in the process, the administration in Washington prescribed that ICANN shall not be subject to the control of states or international organisations.[48] The contradiction that the United States, as a state, stipulates that ICANN should not be subject to state control is obvious. In addition, the United States maintained a special form of influence in that ICANN, as a private company under Californian law, remains subject to the jurisdiction of the United States.

So far, the United States has not openly made use of this influence. However, the meaning of the institutional arrangement became apparent in the sum-

46 On this point, see the "Base Registry Agreement" for new gTLDs, specification 6, paragraph 1.6, p. 78, https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.pdf (accessed 24 April 2019).

47 Jack Goldsmith, *The Failure of Internet Freedom* (New York, 2018), https://knightcolumbia.org/content/failure-internet-freedom (accessed 14 March 2019).

48 Milton Mueller, "The IANA Transition and the Role of Governments in Internet Governance", *IP Justice* (2015): 1—18.

mer of 2018, when the National Telecommunications and Information Administration (NTIA) publicly raised the question of whether the "IANA transition" should be reversed in line with the national interests of the United States.[49] At present, it does not seem that this step will actually be taken, but here, once again, the de facto balance of power with regard to ICANN became very clear.

For countries such as Brazil, Cuba, Russia, and Saudi Arabia, this special position of the United States is in itself a reason to continuously criticise ICANN's role in today's Internet governance. China is less known for open criticism of ICANN. However, the "International Strategy of Cooperation on Cyberspace", published by Beijing in 2017, very clearly calls for equal participation of all states in Internet governance. Among other things, it explicitly refers to the administration of the DNS root zone.[50]

Box 5
gTLDs and ccTLDs, registries and registrars

The DNS connects domain names with IP addresses (see Box 2, p. 12). For a uniform DNS, it is crucial that each domain name is assigned only once. ICANN delegates the allocation of TLDs to registries (such as DENIC for .de and Verisign for .com). However, the registries do not assign individual domains (such as example.com), but delegate this task to registrars.

Today, there are essentially two types of domain names. For all officially recognised states, there are country-code top-level domains (ccTLDs) such as .de and .fr. These are usually administered by a registry in the respective country. In addition, there are numerous gTLDs such as .com and .org. They are not geographically assigned; the respective registries, too, are distributed globally.

WHOIS and European General Data Protection Regulation

ICANN and the EU have been in conflict for several years over the future of the WHOIS system. Put simply, WHOIS is a protocol that allows for making inquiries about the owners or operators of domains. In accordance with the decentralised structure of the DNS, WHOIS is also organised decentrally. The registry responsible for a domain (see Box 5) usually also operates the respective WHOIS system, as for example the German Network Information Center (DENIC), which is responsible for the .de domain. Registries for ccTLDs are usually located in the country whose domain they administer and are therefore subject to the corresponding legal requirements. However, it is controversial as to which requirements should apply to gTLDs.

The EU demands that the data of the owners of gTLDs also be treated in accordance with the European General Data Protection Regulation (GDPR). With this, it clearly expresses its claim to regulate ICANN when it comes to the "European" Internet. ICANN, on the other hand, is clearly unwilling to comply with the provisions of the GDPR. Although it had long been anticipated that the WHOIS regime for gTLDs would be incompatible with the GDPR, ICANN only reacted shortly before the end of the transitional phase for the introduction of the GDPR in May 2018. An interim solution was introduced for an initial period of one year; this is to be replaced as soon as possible by a permanent GDPR-compliant solution.[51]

However, what such a solution should look like has so far been controversial, both within ICANN's bodies and in exchanges with the EU. The United States, but also many other states represented in ICANN's Governmental Advisory Committee (GAC), are insisting that law enforcement agencies in particular should have access to the personal data of those who have registered domains.[52] However, it remains unclear according to which criteria and by which means this access should be granted to law en-

49 Kieren McCarthy, "US Govt Mulls Snatching Back Full Control of the Internet's Domain Name and IP Address Admin", *The Register*, 5 June 2018, https://www.theregister.co.uk/2018/06/05/us_government_icann_iana/ (accessed 14 March 2019).

50 Ministry of Foreign Affairs of the People's Republic of China, "International Strategy of Cooperation on Cyberspace (2017)", 1 March 2017, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/ t1442390.shtml (accessed 14 March 2019).

51 Matt Serlin, "The EPDP on Generic Top-Level Domain Registration Data: Phase 1 Down, Phase 2 To Go", *CircleID*, 28 March 2019, http://www.circleid.com/posts/20190328_epdp_on_gtld_registration_data_phase_1_down_phase_2_to_go/ (accessed 18 April 2019).

52 See, e.g., "Remarks of Assistant Secretary Redl at IGF-USA 2018", 27 July 2018, https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-igf-usa-2018 (accessed 21 August 2018).

forcement agencies — and whether this can be done in a way that meets the requirements of the GDPR.[53]

The Role of States in the Allocation of Domain Names

ICANN has a number of bodies and procedures in place to facilitate broad stakeholder participation in the spirit of multi-stakeholder governance. This also includes states. They can become members of the organisation's GAC and thus participate, in an advisory capacity, in ICANN's decisions.[54]

By now, it is widely accepted in practice that states should be involved in all questions of political importance with regard to "their" domains, that is, the ccTLDs. However, it is highly controversial as to what influence they should have on the allocation of gTLDs. This is currently manifested in three conflicts:[55]

- *2-character country/territory codes at the second level:* This dispute does not apply to ccTLDs such as .de. Rather, it is about the second level of gTLDs, such as .edu and .xxx. A "2-character country code" would take the form .de.edu, for example. Through the GAC, a number of states are now insisting on being involved in the allocation of these domains or, if deemed necessary, on having the possibility of administering the domains themselves at low cost.
- *New gTLDs:* Time and again, there have been contentious cases in which states have demanded a say in the allocation of specific gTLDs. The dispute over the gTLD .amazon, for example, is currently attracting much attention. The US corporation Amazon applied for the gTLD a long time ago but has met with sustained resistance from the countries bordering the Amazon. All attempts by the ICANN Board of Directors to mediate in this matter have so far failed.[56]
- *Intergovernmental organisation identifiers:* For several years now, the GAC has been insisting that the interests of international organisations such as the International Committee of the Red Cross be taken into account and, in particular, be given special consideration when allocating domains of interest to these organisations, also beyond the .int domain.

From the outside, it may seem difficult to understand how such details can spark years of political debate. In fact, however, for some states, fundamental matters are at stake. They want to establish legal mechanisms within ICANN's structures that recognise, and secure, their claim to authority over "their" part of the Internet.

ITU: Blockade

The origins of the International Telecommunication Union go back to the founding of the International Telegraph Association in 1865. In 1932, the organisation took on its present name, and since 1949, on the basis of an agreement with the United Nations, it has functioned as a UN special organisation. The ITU essentially consists of three organisational units: ITU-R for radio communications, ITU-T for standard-setting in telecommunications, and ITU-D for technical assistance and development in telecommunications.

These structures of the ITU have already shown that, so far, the Internet has not been among the main issues dealt with by the ITU. In fact, since the late 1990s, there has been a continuing dispute about whether the ITU should be assigned greater responsibility for global Internet governance issues. In 1997, together with other institutions such as the Internet Society, the ITU was close to issuing seven new TLDs (see Box 5, p. 23), and to assuming direct control of the .int domain. However, this met with strong resistance from the United States, which — not least in

53 Farzaneh Badii and Milton Mueller, *Stacking the Deck? The ePDP on the Whois Temp Spec* (Internet Governance Project, 3 July 2018), https://www.internetgovernance.org/2018/07/03/stacking-the-deck-the-epdp-on-the-whois-temp-spec/ (accessed 4 July 2018).

54 See ICANN, *Bylaws for Internet Corporation for Assigned Names and Numbers (ICANN), as Amended 18 June 2018*, Section 3.6, (a), (III), https://www.icann.org/resources/pages/governance/bylaws-en (accessed 14 March 2019).

55 See ICANN GAC, *GAC Communiqué ICANN 63 – Barcelona, Spain*, 25 October 2018, https://gac.icann.org/advice/communiques/icann63%20gac%20communique%CC%81.pdf (accessed 12 November 2018).

56 Monika Ermert, "ICANN setzt Galgenfrist für .amazon", *heise online*, 14 March 2019, https://www.heise.de/newsticker/meldung/ICANN-setzt-Galgenfrist-fuer-amazon-4335195.html (accessed 14 March 2019).

Box 6
The Plenipotentiary Conference 2018 in Dubai

The negotiations on Resolution 102 during the ITU's Plenipotentiary Conference 2018 in Dubai exemplify the impasse in the ITU. The title of this resolution, which was first adopted in Minneapolis in 1998, is unwieldy, but informative: "ITU's role with regard to international public policy issues pertaining to the Internet and the management of Internet resources, including domain names and addresses". The resolution essentially touches on the question of what role the ITU should play with regard to the Domain Name System.

As is to be expected, supporters of the current model of Internet governance are seeking to reaffirm the role of institutions such as ICANN. To this end, since 2010, the first paragraph of the resolution's decision section has committed the ITU to working with the relevant Internet governance organisations. A footnote explicitly mentions ICANN, the Regional Internet Registries (RIRs), the IETF, the Internet Society, and the W3C.[a]

Since the Plenipotentiary Conference 2014 in Busan, however, the resolution also contains a passage that clearly affirms the states' claim to "their" domains, that is, the ccTLDs.[b] In the run-up to the 2018 conference, the Group of Arab States presented an amendment aimed at extending this right to gTLDs. Also, the preamble of the resolution was to criticise that state interests were not being sufficiently taken into account in ICANN's decisions.[c] The Group of European States, on the other hand, proposed opening up the ITU Council Working Group Internet (CWG Internet) to non-governmental actors, in line with the multi-stakeholder approach and going beyond selective consultations.[d] Ultimately, neither of the two proposals reached the necessary consensus in Dubai.

a International Telecommunication Union (ITU), *Final Acts of the Plenipotentiary Conference, Guadalajara 2010*, 2010, Resolution 102, Resolves 1.
b ITU, *Final Acts of the Plenipotentiary Conference, Dubai 2018*, 2018, Resolution 102, Resolves 4.
c ITU, *Coordinated Proposals Received from ITU Member States for the Work of the Conference, 27 October 2018*, 2018, Resolution 102, ARB/72A1/8, noting with concern b).
d Ibid., Resolution 102, EUR/48A1/8, Resolves 5.

order to avoid such an expansion of the ITU's activities — pushed the establishment of ICANN in 1998.[57]

57 Jill Hills, *Telecommunications and Empire* (Urbana, IL, 2007), 140ff.

Since then, the state of the conflict has not changed. The Western states, led by the United States and the United Kingdom, are strictly opposed to extending the activities of the ITU to the area of Internet governance. Countries such as Russia, China, Brazil, and Saudi Arabia, on the other hand, are trying to assign the organisation a central role in global Internet governance.

The proponents of a stronger role for the ITU primarily emphasise its legitimacy. They argue that, unlike the case of ICANN, the ITU's decisions are the result of inclusive negotiations between all states.[58] Western states, on the contrary, stress that the mandate of the ITU is limited to technical issues, and thus unsuitable for genuinely political decisions. Also, the concern that strengthening the ITU would give authoritarian states such as China, Russia, and Saudi Arabia too much influence on the future development of the Internet is hardly being concealed.[59]

The long-running dispute over the role of the ITU in Internet governance is shaped by three institutional characteristics of the organisation.

First, the meetings of the ITU's highest decision-making body, the Plenipotentiary Conference, take place only every four years. Each of these meetings is therefore of particular importance. Second, all decisions at the ITU must be taken by consensus. This gives the supporters of the status quo, that is, the Western states, a discernible tactical advantage in negotiations. For the most part, they can limit themselves to preventing any expansion of ITU competencies in the field of Internet governance. Third, the negotiations in the ITU are shaped by the fact that, on the one hand, the states negotiate in their own name and, on the other hand, they also partly act as members of regional groups. The latter sometimes exceed the boundaries of the usual political camps, as they

58 Daniel Kennedy, *Deciphering Russia. Russia's Perspectives on Internet Policy and Governance* (London: Global Partners Digital, November 2013), https://www.gp-digital.org/wp-content/uploads/pubs/FINAL%20-%20Deciphering%20Russia.pdf (accessed 14 March 2019); Dave Burstein, "A Closer Look at Why Russia Wants an Independent Internet", *CircleID*, 15 December 2017, http://www.circleid.com/posts/20171215_closer_look_at_why_russia_wants_an_independent_internet/ (accessed 19 December 2018).
59 See, for example, Michael O'Rielly, "Reining in UN's Little Known International Telecommunication Union", *TheHill*, 8 August 2018, http://thehill.com/opinion/technology/400990-reigning-in-uns-little-known-international-telecommunication-union (accessed 13 March 2019).

have their origins in the technical coordination of regional telecommunications networks. Russia, for example, is part of the group of European states organised in the European Conference of Postal and Telecommunications Administrations (CEPT).

Two, Three, Multiple Internets?

We have become used to the idea that there is *one* Internet. For some time now, however, there have been warning signs that the Internet might split up. There is a lot of talk now about "fragmentation" and "balkanisation" as well as the threat of "splinternets".[60] There is widespread concern that the Internet will be divided between the United States and China. Eric Schmidt, for example, one of the founders of Google, commented: "I think the most likely scenario now is not a splintering, but rather a bifurcation into a Chinese-led internet and a non-Chinese internet led by America."[61]

A real fragmentation of the Internet would have to be feared if it came to a split at the infrastructure level.

With a similar thrust, French President Macron, in his opening speech at the IGF 2018, distinguished between a Californian and a Chinese version of the Internet.[62] For Macron, this calls for an independent European path. Conversely, from an American perspective, the regulatory reach of the European GDPR is sometimes interpreted as a sign of a further division of the Internet.[63]

The rhetoric is as diverse as the empirical phenomena at issue in this debate. The analysis in the previous sections suggests two differentiations. First, it is necessary to take a closer look at the level at which fragmentation of the Internet is observed, or feared. At the level of Internet services, it has long been a practical reality that regulatory differences exist along the boundaries of state jurisdiction. More and more states are trying to regulate "their" part of the Internet. This shows the persistence of the principle of territorial statehood.

However, it is misleading to describe these fault lines at the level of Internet services as fragmentation of "the" Internet. At least so far, government regulation of Internet services has been based on a globally shared Internet infrastructure of common standards and protocols. A genuine fragmentation of the Internet would only have to be feared if it came to a split at the infrastructure level. The Domain Name System, that is, the address system of the Internet (see Box 2, p. 12), is of particular importance here, as are basic protocols for data transmission.[64]

With regard to the logical infrastructure, a further distinction must then be made between the different actors driving the trend towards fragmentation. On the one hand, these are the states. The question here is if, in the long run, they will be "satisfied" with regulating the level of Internet services, or if they will extend their claim to regulation to the level of the global Internet infrastructure. There have been repeated statements from China in particular, but also from Russia, emphasising that, for them, alternatives to the DNS currently administered by ICANN are conceivable. The technical organisation of the Internet in

60 See Milton Mueller, *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*, (Cambridge, UK, 2017).

61 Lora Kolodny, "Former Google CEO Predicts the Internet Will Split in Two — and One Part Will Be Led by China", *CNBC*, 20 September 2018, https://www.cnbc.com/2018/09/20/eric-schmidt-ex-google-ceo-predicts-internet-split-china.html (accessed 14 March 2019).

62 Internet Governance Forum, "IGF 2018 Speech by French President Emmanuel Macron", 13 November 2018, https://www.intgovforum.org/multilingual/content/igf-2018-speech-by-french-president-emmanuel-macron (accessed 13 December 2018).

63 The Editorial Board, "There May Soon Be Three Internets. America's Won't Necessarily Be the Best", *The New York Times*, 15 October 2018, https://www.nytimes.com/2018/10/15/opinion/internet-google-china-balkanization.html (accessed 6 November 2019).

64 See also Mirko Hohmann and Thorsten Benner, *Getting "Free and Open" Right. How European Internet Foreign Policy Can Compete in a Fragmented World* (Berlin, June 2018), 36.

Box 7
Tor as an alternative address system

The Tor Onion Service Protocol is an example of an alternative address system. The development of this protocol was originally funded by the Office of Naval Research and the Defense Advanced Research Projects Agency (more commonly known as DARPA), that is, two US military research institutes. Today, however, the protocol is viewed with criticism because it is a component of the so-called dark net.[a] Tor is used to enable a mostly anonymous exchange of data via multiple encryption processes. For one thing, this allows anonymous access to websites on the "normal" Internet based on the DNS administered by ICANN. In addition, there is a special address format for Tor's own "hidden services" that ends with the .onion domain. Although this domain is recognised by the IETF as a special-use domain, it cannot be accessed via the usual DNS system.[b] In order to access addresses within the domain, a special browser is required that can forward the corresponding address requests within Tor's own network.

a See Matthias Schulze, *Kriminalitätsbekämpfung im Dark Net. Neue Ermittlungsansätze statt Verbote*, SWP-Aktuell 28/2019 (Berlin: Stiftung Wissenschaft und Politik, April 2019).
b Jacob Appelbaum, *The ".onion" Special-Use Domain Name*, Request for Comments: 7686, (Internet Engineering Task Force, October 2015), https://tools.ietf.org/html/rfc7686 (accessed 11 March 2019).

China offers a blueprint for this. The Chinese Internet already represents a largely closed intranet that is only connected to the rest of the Internet via state-controlled accesses. Indeed, it is even conceivable that China could include further states in this system, for example within the framework of the still vague ideas of a "digital silk road".[65] Russia has also announced its intention to test decoupling the Russian Internet from the global Internet.[66] The "Law on the Sovereign Internet", passed by the Duma in April 2019, provides the basis for this and also contains references to the goal of building a Russian DNS.[67] Moscow has stated that its aim is to ensure that it is not dependent on the United States in the event of a conflict. However, it is also clear that this will create the basis for extending the state's control over the "Russian" Internet to the infrastructure level — very similar to what is happening in China.

However, a threat to the common global Internet infrastructure is also coming from a completely different direction, namely from private companies, especially those in the United States. As mentioned above, Google and Mozilla, that is, the companies behind two of the most important Internet browsers, are attempting to address the security gaps of today's DNS on their own (see p. 16). To this end, they provide the verification and encryption of DNS queries. This is still done on the basis of the global DNS system administered by ICANN. However, it is conceivable that, in the future, the link to the global DNS will become weaker. Especially for a company as influential as Google, it might be tempting for it to create its own Internet that is only loosely connected to the rest of the web.

For now, such far-reaching considerations are only speculative. But they do give cause for concern. It would not lead to the collapse of all global communication if the Internet were to be split up at the infrastructure level. Certainly, technical ways could be found to enable an exchange across the borders of different networks — just as it is feasible today to connect to the Internet in China or to services within the Tor network (see Box 7). The immediate result, however, would be a considerable shift of power in favour of the gatekeepers. Already today, states and private companies are trying to control what happens within "their" sub-networks. However, most of this is still happening at the level of Internet applications — and on the basis of a shared infrastructure, which at least partly is beyond their control. Citizens are using the remaining freedom to evade state censorship in ever newer ways. Even powerful companies cannot

65 For a similar scenario, see also Marcel Dickow, "EurasiaNet — How They Split the Internet", in *Conceivable Surprises. Eleven Possible Turns in Russia's Foreign Policy*, ed. Sabine Fischer and Margarete Klein, SWP Research Paper 10/2016 (Berlin: Stiftung Wissenschaft und Politik, October 2016), 43—46. See also Milton Mueller, "Proposed New IETF Standard Would Create a Nationally Partitioned 'Internet'", *Internet Governance Project*, 18 June 2012, https://www.internetgovernance.org/2012/06/18/proposed-new-ietf-standard-would-create-a-nationally-partitioned-internet/ (accessed 5 February 2019).
66 Markus Ackeret, "Russlands Internet soll von der Welt isoliert werden", *Neue Zürcher Zeitung*, 12 February 2019, https://www.nzz.ch/international/russlands-politiker-traeumen-von-der-abschottung-des-russischen-internets-ld.1459253 (accessed 14 February 2019).
67 Christina Hebel, "Entscheidung des Parlaments: Wie Russland sich vom Internet abkoppeln will", *Spiegel Online*, 11 April 2019, https://www.spiegel.de/netzwelt/netzpolitik/russland-parlament-billigt-gesetz-zum-abkoppeln-des-eigenen-internets-a-1262345.html (accessed 18 April 2019).

prevent competitors from challenging them on the basis of a common technical infrastructure. If, however, states or companies were to control the infrastructure level too, they would be in a position to close down these remaining spaces of freedom.

Somewhat surprisingly, the fragmentation of the Internet thus carries with it the threat of a further concentration of power. Although today's global Internet infrastructure eludes control by individual actors through various checks and balances, the trend towards separate networks — each with its own distinct infrastructure — is poised to increase the power of gatekeepers, be they states or private companies.

Recommendations for German Internet Governance Policy

The conflicts over the infrastructure of the Internet are deeply political, as they affect the central interests of modern societies. Countries such as the United States, China, and Russia have recognised this and are pursuing their own interests in a very strategic manner. In Germany, on the other hand, an in-depth discussion on this topic is still lacking. The following considerations are intended to contribute to the necessary debate.

The Strategic Context

As explained above, the political debate over the global Internet infrastructure is characterised by a confrontation of two groups. One is led by the United States and aims to defend the current arrangements in global Internet governance. This group, however, is confronted with the increasingly self-confident and strategic activities of states such as China, Russia, and Saudi Arabia. Germany is traditionally part of the camp led by the United States.

A political strategy must take this polarisation seriously. Particular attention should be paid to those states that cannot (yet) be clearly placed in one of the two groups. To this end, a recently published study by the think tank New America identifies 50 states as potential allies of the United States, including Brazil, Singapore, and Serbia.[68] From a German perspective, such a list would likely look different, at least to a certain extent. However, the crucial point is that, for all the confrontation in Internet governance, there are a large number of states somewhere between the two poles. New America aptly describes them as "digital deciders".

Also, in the long run, the advocates of a "liberal" Internet will not be able to limit themselves to defending the status quo. To be sure, they have a certain advantage: Because they shaped the early development of global Internet governance, they were largely able to realise their political aspirations. So far, they have not had to push for change themselves but have been able to defend the current state of affairs. Moreover, the special position of the United States vis-à-vis ICANN and the consensus principle in the ITU made it easy in the past to block unwelcome change.

In the future, however, it will not be enough to rely on this strategic advantage. The idea of a "liberal" Internet must be constantly developed. As described in the previous sections, it is necessary to adapt the global technical infrastructure in key respects to new requirements and changing security threats. Political controversies have already arisen within the liberal camp. For example, it was only in September 2018 that the United States and its allies from the "Five Eyes" intelligence alliance once again insisted that telecommunications companies must give them the opportunity to bypass the encryption of the services offered by the companies ("lawful access").[69] It is particularly in liberal states that the question arises as to how the power of large digital companies can be democratically contained.

If the liberal camp does not succeed in solving the problems of the global Internet infrastructure in a

68 Robert Morgus, Jocelyn Woolbright and Justin Sherman, "The Digital Deciders. How a Group of Often Overlooked Countries Could Hold the Keys to the Future of the Global Internet", *New America*, last updated on 23 October 2018, https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/ (accessed 11 December 2018).

69 Carolin Gißibl, "Angriff der ›Five Eyes‹ auf verschlüsselte Chats und Anrufe", *Süddeutsche Zeitung*, 11 September 2018, https://www.sueddeutsche.de/digital/datensicherheit-verschluesselung-five-eyes-1.4124671 (accessed 14 February 2019). See also Monika Ermert, "Banken und Geheimdienste wollen die Krypto-Hintertür", *Süddeutsche Zeitung*, 2 June 2019, https://www.sueddeutsche.de/digital/tls-verschluesselung-1.4317326 (accessed 14 February 2019).

way that, at the same time, is at least acceptable to other states, there is a risk of the fragmentation of this very infrastructure. Even more than they are doing today, states, regions, and companies will try to find their own solutions for "their" area of the Internet. In this context, those states that have not yet sided with one of the two groups will have a special role to play. If they get the impression that liberal states block any change to the status quo, this could increase the attractiveness of alternative offers from states such as China and Russia.

Priorities

German policy in the field of Internet governance has so far been guided by five goals (see p. 8f.): promoting the digital economy (#Z1); strengthening the security of IT systems (#Z2); protecting human rights in the digital space (#Z3); strengthening multi-stakeholder governance (#Z4); and preserving global interoperability (#Z5).

The analysis of the current lines of conflict suggests that priorities need to be set. The disputes both at ICANN and in the ITU show that there is no prospect in the foreseeable future for an agreement on politically charged further developments of the Internet infrastructure at the global level. With regard to economic issues, human rights, and security (#Z1, #Z2, #Z3), the differences between the states are simply too great. Moreover, as described above, the current model of multi-stakeholder governance (#Z4) reaches its limits precisely when it comes to such genuinely political questions. This does not mean that Germany should not continue to stand up for these goals. However, it should be acknowledged that these goals will not be achievable in the near future at the level of the global Internet infrastructure.

In fact, on the global level it seems necessary to first of all defend the achievements of the past. The goal of interoperability (#Z5) thus comes to the fore. As described above, in the future, it can no longer be taken for granted that there will be a technically unified and globally interconnectable Internet infrastructure. If states or companies create technically independent networks, there is a risk of a problematic shift of power in favour of the respective gatekeepers. This in turn would in all likelihood have negative effects, both on economic development (#Z1) and on the protection of human rights (#Z3). It is therefore necessary to defend the fragile consensus to hold on to a common foundation of the Internet.

However, pursuing the goal of global interoperability on its own stands in a certain tension with the problem diagnosis developed so far. The aforementioned political problems of the Internet infrastructure are not solved by adhering to technical interoperability. In addition, therefore, Germany should promote updates of its own logical infrastructure — without thereby further contributing to the Internet's fragmentation. The EU provides a suitable framework for this. In principle, it is possible here to authoritatively set new standards, for example on privacy in the DNS system. What is crucial here is that such additions to the logical infrastructure do not end up further undermining the global Internet infrastructure but, instead, complement it.

This twofold orientation towards global interoperability and regional updates of the Internet's logical infrastructure can be translated, in the next step, into three practical recommendations for German Internet governance policy.

Restricting ICANN to Its Core Technical Functions

A unified DNS is one of the essential prerequisites for global interoperability. There is a need for an authority to assign "names and numbers", that is, domain names and IP addresses. In principle, this exercise of authority is widely considered legitimate for functional reasons: ICANN's rules are recognised because almost all the actors involved see the need for such an institution.

However, as described above, this functional legitimacy reaches its limits in cases where ICANN moves into the realm of politically controversial issues. This clearly shows that the organisation, despite all its efforts for transparency and participation, does not have sufficient legitimacy to make genuine political demands. At the international level, state approval is widely regarded as the most important source of legitimacy. As a private institution, however, ICANN cannot obtain this kind of approval; even its GAC, in which states can become members, is explicitly supposed to have only an advisory function.

ICANN's activities should, as far as possible, be limited to those technical functions that are widely recognised as legitimate.

However, if ICANN cannot generate more legitimacy, it seems prudent to shield it from unrealistic expectations. This would mean restricting ICANN's activities as far as possible to those functions that are widely recognised as legitimate. This includes in particular the authoritative management of the DNS root zone — that is, the hierarchical top of the DNS — as an essential prerequisite for global interoperability (see Box 2, p. 12).

This position is not uncontroversial and would have to be proactively promoted. A good starting point for this is the GAC. Germany is represented here and could coordinate its activities with other EU states. In addition, it would not be improper to also try to convince German companies involved in ICANN to support this policy.

With regard to ccTLDs, a certain political division of labour has already developed that fits with the idea of restricting ICANN to its core technical functions. The GAC is granted a special role when it comes to political issues concerning ccTLDs, and it is recognised that the registries responsible for ccTLDs (see Box 5, p. 23) are subject to the jurisdiction of the respective states, for example that DENIC — the registry for the .de domain — is subject to German law.

However, it is more difficult to limit ICANN to core technical functions as far as the allocation and operation of gTLDs are concerned. The problem with the allocation of a gTLD such as .amazon is that, in such cases, it is disputed which registry may administer a domain. As long as it remains unclear which registry is responsible, it also remains unclear under what jurisdiction the domain falls. The usual ccTLD division of labour between ICANN and the states is therefore not possible here. There is also no global institution with the authority to resolve conflicts, as in the case of the .amazon domain, in a way that is binding for all parties involved. Therefore, such disputes will have to be dealt with by ICANN itself in the future. With the Uniform Domain-Name Dispute-Resolution Policy, ICANN has long since developed a procedure for this purpose that is intended to take into account the interests of all parties involved. In the end, however, in certain cases decisions will be made whose political significance is not sufficiently covered by ICANN's technical and functional legitimacy.

In order to alleviate this problem at least to some extent, Germany should, through its involvement in the GAC, support existing efforts to make decision-making processes at ICANN more transparent. In many ways, the organisation is already very transparent. However, the multitude of procedures, procedural rules, and stakeholders makes it an extremely challenging task to evaluate the publicly available information. This is a particular problem for representatives of civil society, but also for many states. In order to increase acceptance of ICANN's core functions, Germany should accordingly support initiatives to improve ICANN's transparency, particularly with regard to the allocation of gTLDs.

Once gTLDs have been allocated, it would be appropriate, in view of the operation of these domains, to aim for a political division of labour that frees ICANN from having to make insufficiently legitimate decisions. In this sense, Germany could work within the GAC to defuse two conflicts that have been simmering for some time:

- The first case concerns the current debate on the WHOIS system for gTLDs (see p. 23). Here, in particular, it seems appropriate for ICANN to hold back. Instead of creating a universal WHOIS system, ICANN should oblige the registries of gTLDs to transparently state which jurisdiction they are subject to and to provide a WHOIS system in line with that jurisdiction's requirements. The gTLD .audi, for example, is operated by Audi AG. ICANN should thus require the company to create a WHOIS system that complies with German and European data protection law. If law enforcement agencies from other countries also wish to gain access to publicly inaccessible data, the usual means of requesting legal assistance are available to them. Such instruments may seem too slow to many law enforcement agencies in the age of digital communication, as the current discussions about the US CLOUD Act and the European "E-Evidence" package make clear. But it is precisely here that we can see how highly political questions of digital evidence are. ICANN simply does not have the legitimacy to provide authoritative answers here.
- In the dispute over second-level "2-character country codes", German policy could also seek to de-escalate (see p. 23). As described above, this controversy can be understood as an attempt by some states to extend their authority beyond ccTLDs to the area of gTLDs. However, there is still no proof

that important interests of the states are affected. For example, it has always been common for websites to be designed in German or to use a .de domain without being operated by a German provider. Here, too, in serious cases, states have the option of turning to the relevant registries for legal assistance. If German policy is interested in maintaining ICANN's core function, it should therefore actively advocate freeing the organisation from the burden of a political controversy that has predominantly symbolic content, and thus serves precisely to question ICANN's legitimacy.

Public Support for Multi-stakeholder Institutions in the ITU and the IGF

For systemic reasons, non-state governance reaches its limits when it comes to political conflicts. Despite these limits, the current model of Internet governance also has its strengths. Multi-stakeholder institutions such as the IETF, the IEEE, and the W3C provide public goods in the form of protocols and standards. In this way, they make a significant contribution to maintaining and further developing the global Internet infrastructure. In addition, despite all the criticism in detail, it is certainly an impressive achievement that ICANN reliably provides a uniform global DNS. While remaining conscious of the limits of non-governmental governance, German policy should therefore offer these institutions political support wherever they can play to their strengths.

In doing so, Germany should see the relevant institutions of the United Nations as important places for global political debate. For different reasons, the IGF and the ITU themselves are not suitable for resolving the conflicts surrounding the global Internet infrastructure (see p. 22ff.). It should not be underestimated, however, that these institutions create forums in which (still) almost all states come together to exchange views on issues of global Internet governance. The IGF, moreover, provides an institutional framework in which states regularly and systematically meet with representatives of business and civil society.

Germany should use these forums to promote the importance of multi-stakeholder institutions such as ICANN, the IETF, and the W3C. The conditions for this are good. As the third-largest contributor to the ITU and the host of the IGF 2019, Germany has a prominent role in both fora.

In this process, Germany should avoid contributing to the stark confrontation between the two groups described above and, instead, should take up constructive criticism of the existing institutions of global Internet governance. This would send an important signal to those states that express such justified criticism. As in the case of ICANN, the challenge for institutions such as the IETF, the IEEE, and the W3C is to create meaningful transparency. In addition, the fact that companies play a dominant role in these institutions deserves attention (see p. 10). In order to reduce this problem to at least a tolerable level, the participation of civil society and science should be strengthened.

Germany should also be more consistent in its domestic and foreign policy. Both at the level of the Internet infrastructure (e.g. broadband expansion, 5G) and at the level of Internet services (e.g. Network Enforcement Act), the German government has the chance to demonstrate what kind of multi-stakeholder involvement it deems appropriate — and also, where it sees the limits of participation by non-state actors.

Updates to the Internet Infrastructure on the European Level

The previous recommendations have focussed on how Germany can use its influence in ICANN, the ITU, and the IGF to pursue the goal of preserving global interoperability. The political effort to maintain a common technical infrastructure at the global level will not, however, resolve the conflicts about the further development of this infrastructure. On the contrary, the price of maintaining global interoperability will likely be to accept, at least for the moment, that these conflicts will not be addressed. However, if global solutions to these conflicts — and the underlying cracks in the Internet's foundation — are not attainable in the foreseeable future, Germany should make every effort to promote the search for solutions within the EU.[70]

70 On this point, see also Matthias Kettemann, Wolfgang Kleinwächter and Max Senges, *The Time Is Right for Europe to Take the Lead in Global Internet Governance*, Normative Orders Working Paper 2/2018 (Frankfurt: Goethe Universität, February 2018); Hohmann and Benner, *Getting "Free and Open" Right* (see note 64).

In principle, the EU has clearly positioned itself as a proponent of a "liberal" Internet governance policy. In 2014, for example, Neelie Kroes, then the Commissioner for the Digital Agenda, expressed strong commitment to ICANN and the multi-stakeholder model of Internet governance. Yet, the future of the Internet is controversial also within the EU. With the GDPR, the EU has recently established itself as an advocate of data protection. However, the e-privacy regulation that is supposed to build on the GDPR and formulate rules specifically for digital communication is the subject of fierce debate. There is disagreement both among the member states and between member states and European companies. Also in Europe, law enforcement and security agencies are trying vigorously, both legally and operationally, to find new ways of circumventing encryption procedures for their own purposes. Thus, in order to tackle the structural problems of the Internet infrastructure at the European level, as described above, first of all a lot of persuasion will be needed.

European updates of the Internet's logical infrastructure should complement the global infrastructure – and must not add further to its fragmentation.

The focus on the European level, however, also creates a tension with the goal of global interoperability. In order to prevent this tension from turning into a contradiction, all developments in Europe should complement the global infrastructure — and must not add further to its fragmentation. In the following, the meaning of this requirement is exemplified by returning to the previously analysed conflicts over the global Internet infrastructure.

For instance, measures to increase security and data protection in Europe can be implemented without compromising compatibility with other configurations. The EU could, for example, require European registrars (see Box 5, p. 23) and ISPs to use DNSSEC. At least for all European ccTLDs, this would significantly increase the level of security, as well as for all gTLDs registered in Europe. In a similar vein, the EU could make it mandatory for ISPs to encrypt their customers' DNS requests in an appropriate way (e.g. through "DNS-over-TLS").

The EU could also require European network operators to implement mechanisms to improve the security of the routing system, at least within the EU (see p. 17). This would not solve the problem of the targeted re-routing of data ("BGP hijacking") in its global dimension, but it would increase security for European Internet users. The effect could be further amplified with the additional requirement to prioritise secure routes. To some extent, this proposal builds on the idea of a "Schengen routing" that emerged in 2013 in response to revelations about the NSA's comprehensive surveillance measures. The idea here was to avoid unnecessarily routing connections between two devices in Europe via servers outside the continent.[71] In contrast, the idea proposed here is to prioritise routes not because they are in a certain territory, but because they are sufficiently secured. If necessary, this can include routes beyond Europe — but again, in this model, priority would be assigned to those sub-networks whose routing data is considered to be sufficiently trustworthy.

Finally, Europe could use its economic influence to address the weaknesses of today's network of submarine cables (see p. 18f.). Avoiding particularly vulnerable "chokepoints" — as in the case of Europe's connections to Asia through the Suez Canal — is in Europe's very own interest. The aim here should be to create appropriate incentives for network operators. In addition, however, the EU could also address the inadequate connection of African states to the submarine cable network as part of its development cooperation with these states. For Germany, this would not only fit well with the government's stated goals for its policy towards Africa, but it might also help Germany find new allies in the disputes over global Internet governance.

Europe has the potential to shape the developments in global Internet governance. With measures such as those suggested here, it can advance the further development of the Internet's global infrastructure and ensure that its own political priorities have a place within that infrastructure. To emphasise again, however, such an active European Internet governance policy must be designed very carefully to avoid adding to the fragmentation of the Internet. In light of the goal of global interoperability, all European efforts should thus complement and further strengthen the global foundation of the Internet.

71 Jan-Peter Kleinhans, "Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets", *netzpolitik.org*, 13 November 2018, https://netzpolitik.org/2013/schengen-routing-de-cix-und-die-bedenken-der-balkanisierung-des-internets/ (accessed 11 December 2018).

Abbreviations

BGP	Border Gateway Protocol
BGPsec	Border Gateway Protocol Security
BMWi	Federal Ministry of Economic Affairs / Bundesministerium für Wirtschaft und Energie
ccTLD	Country-Code Top Level Domain
CEPT	European Conference of Postal and Telecommunications Administrations
CWG Internet	Council Working Group Internet (ITU)
DARPA	Defense Advanced Research Projects Agency
DENIC	German Network Information Center / Deutsches Network Information Center
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EU	European Union
GAC	Governmental Advisory Committee (ICANN)
GDPR	General Data Protection Regulation
gTLD	Generic Top-Level Domain
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IGP	Internet Governance Project
IPv4	Internet Protocol Version 4
ISP	Internet Service Provider
ITU	International Telecommunication Union
IXP	Internet Exchange Point
MANRS	Mutually Agreed Norms for Routing Security
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
RIR	Regional Internet Registry
SSL	Secure Socket Layer
TCP/IP	Transmission Control Protocol / Internet Protocol
TLS	Transport Layer Security
W3C	World Wide Web Consortium
WSIS	World Summit on the Information Society