Who Governs the Internet?

The updated and expanded new edition

FRIEDRICH EBERT STIFTUNG

Imprint (German)
1/2020
Friedrich-Ebert-Stiftung
Political Academy
Media Politics
Godesberger Allee 149
53175 Bonn, Germany
www.fes.de/medienpolitik

Responsible for this publication at the FES are
Dr. Johanna Niesyto, Head of FES Media Politics in the Department of Political Academy of the Friedrich-Ebert-Stiftung, and
Katrin D. Dapp, FES Media Politics Officer in the Department of Political Academy of the Friedrich-Ebert-Stiftung.

Responsible for this publication at iRights.Lab is
Philipp Otto, Managing Director
www.irights.lab.de

Authors
Henning Lahmann, Jan Engelmann

Editorial office
Anne Lammers, Jana Maire

Translation
Beatrice Gutmann, Forrest Holmes

Design and typesetting
tigerworx Berlin

Publishing house
Friedrich-Ebert-Stiftung, Bonn

The views expressed in this publication are not necessarily those of the Friedrich-Ebert-Stiftung.

ISBN: 978-3-96250-505-9

Who Governs the Internet?

The updated and expanded new edition

FRIEDRICH EBERT STIFTUNG

Content

Photos (left to right): Mario Sixtus / CC BY-NC-SA 2.0; Kristian Niemi / CC BY-NC-ND 2.0; icannphotos / CC BY-SA 2.0; Gregor Fischer, re:publica / CC BY 2.0; Mario Sixtus / CC BY-NC-SA 2.0

Preface

The internet has emerged as a *global promise of freedom.* Its success as a worldwide communications net work rests upon its liberal and open architecture. The question of who governs the internet is the key question confronting digital society. We continue to search for answers as to how certain areas of the internet could better be regulated and who should be responsible for them. This has been a constant theme since the first edition of this publication: Internet governance, the global regulation of the internet, is and remains a *never-ending quest.*

As early as 2005, Jeanette Hofmann defined internet governance as an "open, collective process of searching, [...] which aims to fill a global regulatory lacuna in a way that is conceptually and institutionally legitimate". The Internet Governance Forum (IGF) plays a central role in this search. The IGF was founded in 2006 by the Secretary General of the United Nations (UN) and emerged from the UN World Summit on Information Society (WSIS). The UN convened this summit between 2002 and 2005 with the original aim of overcoming the global digital divide. The IGF has since developed into the central international forum on the future of internet governance and digital policy, addressing the fundamental questions of the openness and freedom of the internet as well as of access to it. The IGF is an open platform for discussion surrounding the central legal, political, social and technical issues concerning the internet. Its multistakeholder approach brings all relevant social groups to the table, particularly underrepresented voices from developing and newly industrialized countries. The 14th IGF took place for the first time in Germany in November 2019, with the motto "One World. One Net. One Vision."

Unlike other UN formats, the IGF does not make binding decisions. The primary goal is to promote an equitable and constructive dialogue among stakeholders drawn from states, international organizations, academia, business and civil society. The basic approach of the IGF is that various actors from various parts of the world can contribute their own perspectives, discuss these with each other, and thus advance the decision-making processes carried out by other bodies—for example the UN, the Internet Society (ISOC), the Internet Engineering Task Force (IETF), the Internet Corporation for Assigned Names and Numbers (ICANN), the European Union or the International Telecommunication Union (ITU).

The liberal and open architecture of the internet has rarely been under such severe strain as it is today. Following revelations of vast espionage campaigns waged by various secret services and in light of the enormously increasing number of cyberattacks, the need for a discussion about regaining and preserving digital sovereignty is more urgent than ever. *Nonetheless, digital sovereignty must not be reinterpreted as calling into question an open and free global network and instead furthering the establishment of the infrastructure of surveillance and censorship.*

Internet governance concerns us all. For the digital society, much is at stake: access to the internet, human and civil rights, social, societal, cultural and economic participation by all, fair global trade, and confidence that our global "network of networks" is secure at all times. Digital policy is and remains social policy. I would like to thank the Friedrich-Ebert-Stiftung, which with this publication continues to encourage civil society activists, politicians, scientists and citizens to take part in and to further this quest, so that the internet's promise of freedom can be fulfilled.

How should the internet be regulated in order to be an important component of a good society? And who should be responsible?

Dr. Jens Zimmermann, MdB
Digital policy spokesman for the SPD parliamentary group in the Bundestag

Foto-AG Gymnasium Melle / CC BY-SA 4.0


Internet regulation concerns us all!

Photo: Mario Sixtus. Boy in a Bubble (2) / CC BY-NC-SA 2.0

The internet is with us, basically everywhere. While stationary PCs live out their miserable existences almost exclusively within the confines of the office, we have long accustomed ourselves to smartphones in the schoolyard, smart watches on our morning jogs, and voice assistance systems such as Alexa or Siri in our kitchens and living rooms.

In nearly every area of our lives, we rely on the internet. However, alongside the countless advantages it offers, the internet creates almost as many challenges for society—in different ways and to different extents, depending on the country concerned. One thing, however, holds true everywhere: the internet does not evolve of its own accord, and it does not automatically provide a space for citizens to express themselves freely. In order for it to function properly in the technical sense, as well as politically and socially, human intervention and direction is needed. The internet must be regulated, administrated, and governed.

The laws we have to comply with come from the German parliament or from EU institutions. What applies to internet users in Germany does not necessarily also apply to Brazilians who access the internet from Rio de Janeiro.

The internet is global, but decentralized and legally fragmented. Different rules apply depending on where you are when you access the internet. But also the possibilities of access or the level of security when online are by no means the same for everyone. The situation on the net reflects to a certain extent the political situation in any given country. Civil liberties, which EU citizens, for example, take for granted online, may be be barred to users in a state under an authoritarian regime.

The politics of internet regulation can be divided into different fields: infrastructure, development and foreign aid; security; human and civil rights; and legal developments. The key question here is how the different goals of internet regulation should be implemented: via agreements between states or in ways that include all stakeholders? Via binding treaties or loosely drafted cooperation?

In addition to these substantial questions, it is especially important to determine who is to be responsible for the regulation of the internet. Should it be international organizations run by nations, or rather open forums that include members of society and economic actors? This publication sets out to give answers to these very important questions in parallel: Who governs the internet, in what way, and with regard to which fields of action? An attached glossary explains the most important technical terms used in the text.

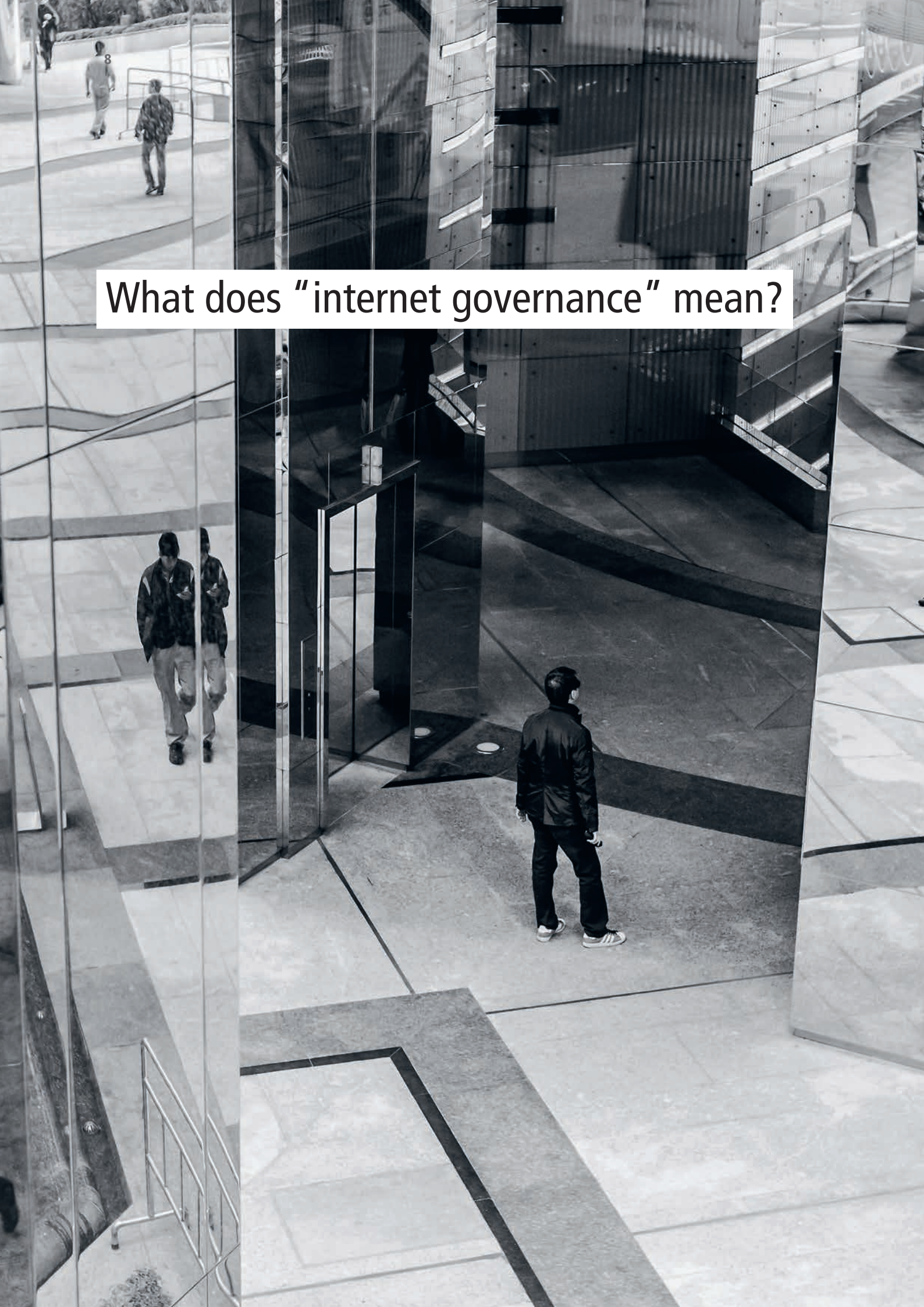
The key questions of internet regulation are:

How can civil liberties be guaranteed on the internet for as many people as possible?

What should global trade over the internet look like?

Who will ensure that the technical infrastructure of the internet continues to function smoothly?

What does "internet governance" mean?



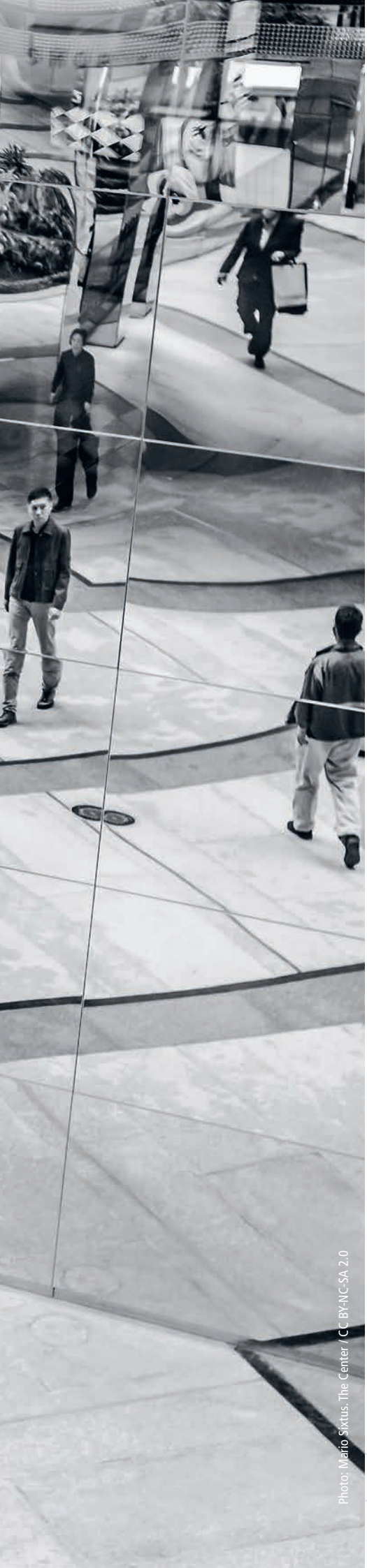


Photo: Mario Sixtus. The Center / CC BY-NC-SA 2.0

What are we talking about when we look at the current and future shape of the internet? What are we talking about when we consider the current and future regulation of the internet? In the English-speaking world, the term "internet governance" has become the standard way to label the policy field described in the preface. It cannot be easily translated into German: In the present understanding, the field designated by this term encompasses "governing," "regulating" and "administering" the internet.

The two core questions of internet governance

It is helpful to divide the topic into two core questions. On the one hand, there is the question of who is to govern the internet, i.e. who is (or should be) responsible for making decisions relating to the internet that are binding for everyone and that affect all users of the net. It is important to understand that the internet is not a single, unified structure, and that, rather, the term denotes a global "network of networks", i.e. a conjunction of many individual networks which communicate with each other electronically. For this reason, the internet does not have a centralized administration or government. Therefore, the entities who are to make decisions regarding the overall structure of the internet will have to be determined and are by no means self-evident. The most important candidates and their respective roles are presented in the third section of this publication.

In addition to the question of *who* is to govern the internet, there is the second question of *what* specifically is to be included in the purview of the different players. The internet is first and foremost a technical structure. However, as mentioned above, no other technology today has such a transformative, lasting impact on our personal and professional lives. Hence it would be short-sighted to restrict the governance of the internet to the administration, extension and technical maintenance of the underlying infrastructure.

The four levels of internet governance

In order to clearly present the different dimensions of the topic of internet governance, it makes sense to consider four different levels that comprise the internet: infrastructure, logic, applications, and content.

— Infrastructure includes the hardware that forms the basic structure of the global net: e.g. all routers, switches, servers and equipment for data transmission such as copper or fiber-optic cables.

— Logic refers to the technical norms and standards that are the preconditions for communication to function on a global scale. These include

Core questions of internet governance:

Internet governance

- **Who** sets the rules?
- **What** is regulated?

resources such as the Internet Protocol (IP), web addresses, domain names, and the corresponding domain name system (DNS).

— Applications are the part of the internet that primarily involves software that allows users to interact with each other and with other systems and websites. The most important and well-known of these applications is the World Wide Web, which can be accessed through internet browsers such as Firefox, Chrome, or Safari.

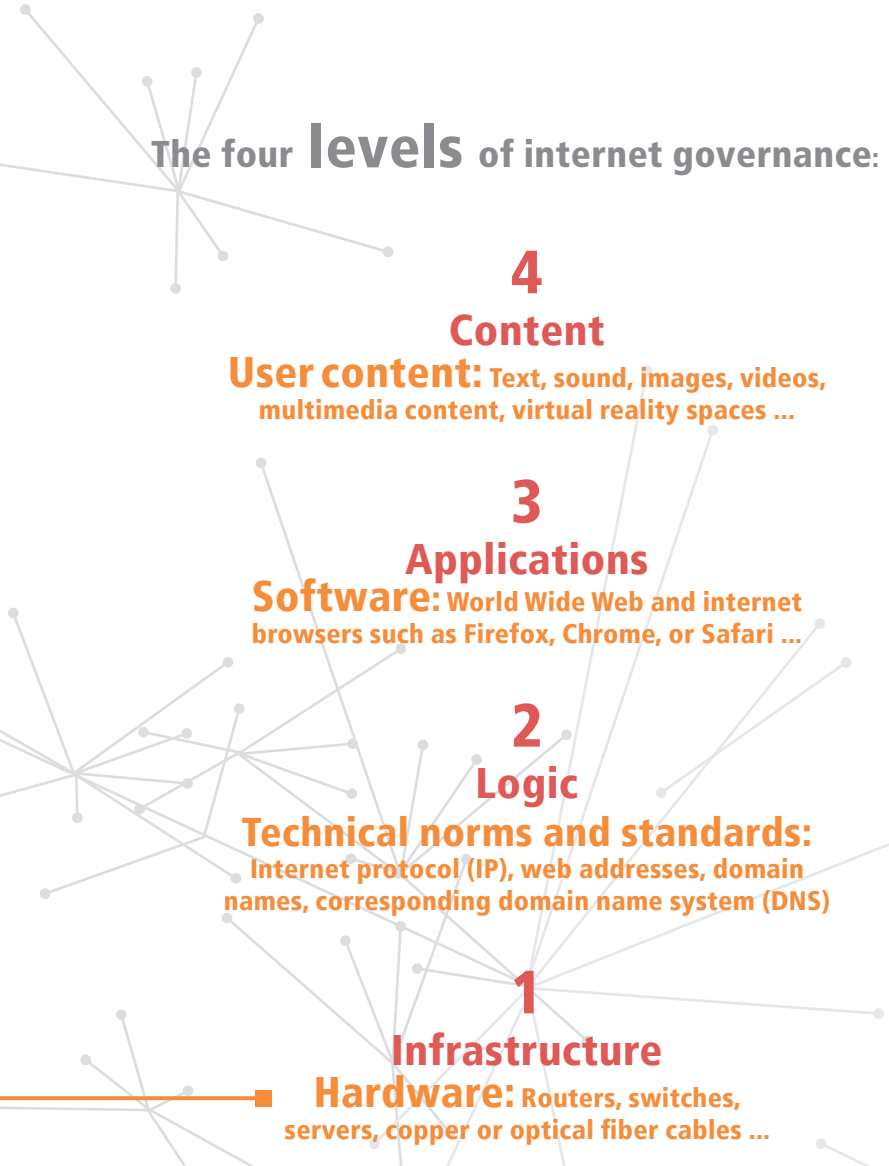
— Content is the level that is most relevant to users. This level includes everything we see or interact with on the computer screen when we "go online", i.e. text, sound, images, videos or other multimedia content, as well as virtual reality spaces or chat bots that engage in dialogue with us.

From the technical to the political regulation of the internet

Initially, in the early days of the internet, internet governance was almost exclusively concerned with the first two levels—infrastructure and logic. The internet was viewed predominantly as a purely technical infrastructure. Hence, the problems that required regulation were primarily technical in nature. With the opening up of the network to commercial and other uses, and with its growing relevance in more and more areas of society, this narrow conception of internet governance has come to be considered insufficient. Currently, most political challenges relating to the internet take place on the level of content, e.g. questions of access to knowledge and culture, or human and civil rights on the internet. Accordingly, it is now generally recognized that internet governance refers to all four levels of the internet. This, however, does not preclude different institutions from being primarily responsible for different levels of internet governance.

With reference to all four levels of the internet, the UN World Summit on the Information Society held in Tunis in 2005 by the International Telecommunication Organisation (ITF), which was attended by some 17,000 participants from 175 countries, attempted for the first time to provide a comprehensive definition of internet regulation, which is still widely used today: It includes "the development and application by governments, the private sector and civil society, in their respective roles, of uniform principles, norms, rules, decision-making processes and programmes shaping the evolution and use of the Internet".

In 2005, the United Nations initiated a worldwide summit, organized by the International Telecommunication Union (ITU), on the topic of "The Information Society." Held in Tunis, about 17,000 participants from 175 countries convened to debate the future of the internet. The summit included an initial attempt to create a comprehensive definition of internet governance relating to all four levels. This definition is still in use today. It encompasses "the development and application of uniform principles, norms, rules, decision-making processes, and programs for the



Three questions for Prof. Dr. Laura DeNardis

Faculty Director of the Internet Governance Lab at the American University in Washington, D.C.

Photo: Centre for International Governance Innovation

"The ecosystem of actors is expanding"

Has the eclectic ecology of the internet turned into something that is significantly influenced by a few technology companies?

Laura DeNardis: The digital world has moved from 2D into 3D and internet governance must as well. The most complex and consequential battles over internet governance are emerging in the cyber-physical world. The internet has leapt from human-facing display screens into the material world of medical devices, home appliances, and industrial cyber-physical infrastructure. This transformation complicates what counts as a technology company—in that all firms are now tech companies—as well as which governance and standards-setting institutions are most relevant.

What do you see as the biggest challenge for good internet governance?

Rather than contracting, the ecosystem of actors is actually expanding. This also complicates the question of internet usage because many "people" online are actually bots and more things than humans are now connected. The embedding of the internet into the physical world heightens already consequential problems concerning privacy, speech, national security, democracy, and consumer safety.

Which main lines of conflict can we expect in the next few years?

An outage is no longer a question of losing access to communication and content, or the digital economy, but about possibly the loss of life or the ability to wage war over the internet and reach into civic infrastructure. At the same time, the security of the internet of things is generally insufficient. The practice and study of internet governance has to rise to meet this generational challenge.

Prof. Dr. Laura E. DeNardis is Professor and Interim Dean of the School of Communication at the American University in Washington, D.C., where she is also Faculty Director of the Internet Governance Lab. With a background in information technology and science and technology studies, she has published six books and numerous articles on the political implications of the technical architecture and governance of the internet. Her latest book, "The Internet is Everything", takes a closer look at the internet of things.

The most complex and consequential battles over internet governance are emerging in the cyber-physical world.

internet, which are carried out by governments, the private sector, and civil society in their respective roles, and which all shape the evolution and use of the net."

A short history of the internet and internet governance

The technical structure we now know as the "internet" was created in the late 1960s as a research project by the US Department of Defense and a number of universities located mainly in California. Between 1984 and 1986, the National Science Foundation (NSF) extended this structure to form a general research network, connecting local networks of American universities for the purpose of exchanging information. Around this time, the term "internet" started coming into use.

The internet spreads around the world

In the 1980s, other countries started connecting to the internet, among them European nations like the Netherlands, Italy, and Germany. Until 1991, the NSF had prohibited any commercial use of the internet; over the following years these restrictions were loosened, and by the middle of the decade, the internet had passed over into private hands. By the end of the century, the internet had grown considerably and commercial uses had become common. At the instigation of the USA, the Internet Corporation for Assigned Names and Numbers (ICANN) was founded in California in 1998. This non-profit organization is still responsible for coordinating the domain name system and for dispensing IP addresses. Essentially, it maintains the technical structure of the internet. As a subunit of ICANN, the Internet Assigned Numbers Authority (IANA) has for decades taken care of basic administrative and technical functions, registering and publishing root name servers and new standards. In 2016, the contract between the US Department of Commerce and ICANN to perform these administrative functions expired and supervision of IANA was transferred to the private sector.

The development of intergovernmental internet governance

As the internet became increasingly commercial, it did so under regulation initially characterized by multilateral agreements between states. As early as 1996, the World Intellectual Property Organization (WIPO) passed the two so-called "internet treaties": the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT). The purpose of these treaties was to adapt the copyright laws of the participating countries for the digital age. Further treaties concerning internet regulation were created by various countries in the context of the World Trade Organization (WTO). These treaties include the GATS Treaty, passed in 1995, which concerns the global market of telecommunications services. Another milestone of international regulation was reached in 2001, when the Council of Europe passed the Budapest Convention, which for the first time addressed the topic of cybercrime in detail.

As the internet became increasingliy commercial it did so under regulation initially characterized by multilateral agreements between states.

From the World Summit to IGF

By the beginning of the 21st century, the crucial role of the internet in global society beyond mere commercial use had become undeniable. In order to do justice to this development, Secretary General Kofi Annan tasked the International Telecommunication Union (ITU), a specialized agency of the United Nations, with organizing a world summit on the topic of "The Information Society" (World Summit on the Information Society, WSIS). It was held in two parts, the first of which convened in Geneva in 2003, and the second in Tunis in 2005. The most important result of the summit was the founding of the Internet Governance Forum (IGF) as a permanent platform for discussing questions involving the regulation of the internet. Out of this has grown a series of annual events that have taken place at different locations since 2006 and are now planned and carried out independently of the UN. At the first IGF meeting in Athens (2006), the various strands of discussion still focused on four central aspects: openness, security, diversity and access. In the years since, the field of topics under discussion has broadened considerably.

Photo: Jason Krüger / CC BY-SA 4.0

Three questions for Prof. Dr. Jeanette Hofmann

Political scientist and internet researcher at the Wissenschaftszentrum Berlin

"There is always room for experimentation with something different"

For years, you have been studying the actors and power mechanisms that shape the politics of the internet. You have come to the conclusion that every time a new field of policy takes institutional shape, it does so around a central good that must be protected. How does this look in the context of internet governance?

Jeanette Hofmann: We should begin by clarifying whether, in the case of internet governance, one can even speak of a new field of policy. Broadly speaking, some characteristics of an emerging policy field can be identified: A problem is perceived, and numerous actors regard this problem as being so important that they set out to address it, meeting again and again to argue about the best solutions. In this case, the problem lay in the still open question of who should set the rules for the internet. Even if they have fundamentally different opinions about the answer to this question, the relevant actors still form a subculture that makes them recognizable as such. This encompasses a technical jargon, a certain expertise, even a brand of humor that at some point becomes distinct. Of course, there have also been ongoing processes of institution building in the field of internet governance: ICANN, the IGF and its national offshoots, and the corresponding areas of responsibility in associations and in national ministries. Nonetheless, I still do not see a consensus around the imperative to protect any one good that is able to mobilize broad societal support. On the contrary, most people are more or less indifferent towards the issue of internet governance, to the degree that they are aware of it at all.

In retrospect, many people see the Snowden revelations as a kind of tipping point in the history of the internet. Have we since entered a new phase in which our primary concern should be minimizing danger, rather than realizing the liberal potential of a global communications space?

The interviews we carried revealed that many experts do actually see, in retrospect, the Snowden revelations as a turning point, because the critical net community in Germany failed to politically leverage the evidence of massive and systematic violations of fundamental rights by state organizations. One member of the Bundestag said that they had failed as a civil rights activist because they were unable to carry out "our Fukushima". From a policy point of view, the ideals that prevail in neighboring policy fields remain dominant: Industry 4.0, AI strategy, but also national security and, more recently, media policy. That a "free and open internet" is a good inherently deserving of protection is a notion that is certainly invoked at times, most recently in the debate around copyright reform, but it lacks the strength to determine a public discourse.

At the moment there is much talk about the use potential of new technologies, e.g. artificial intelligence or blockchain. What chance does civil society have to sound and strengthen divergent perspectives that go beyond purely economic considerations?

There is already a critical discussion around the use of AI, e.g. on the potential for discrimination deriving from biased training data. Regarding blockchain, there is a great deal of skepticism around the libertarian idea that it can level economic or political power. These critical voices are certainly heard by the business community, although they are perhaps not interpreted as many would wish. I believe that the potential for civil society currently lies above all in being able to point to alternatives. Not all search engines, platforms and expert systems follow the same logic. In the shadow of the the major internet firms there is always room for experimentation with something different and unexpected, which, if successful, could disrupt politic's linear, predominant logic of progress.

Prof. Dr. Jeanette Hofmann, Professor of Internet Policy at Freie Universität Berlin, conducts research at the Social Science Research Center Berlin (WZB) on the topics of global governance, regulation of the internet, and digital change. She is also head of the WZB project group "Politics of Digitalization," which investigates the interpretation, negotiation and regulation of digital transformation. From 2010 to 2013 she was an expert in the Enquete Commission "Internet and Digital Society" of the German Bundestag. In 2017, she contributed to the founding of the German Internet Institute, the Weizenbaum Institute for the Networked Society.

The levels of politics and content in internet governance

Assuming that internet governance must not be restricted to the technical administration of network infrastructure, but rather must extend to all four levels of the internet, several issues can be identified that are currently being addressed by internet regulation.

Stability of infrastructure, cooperation, and foreign aid

From a technical point of view, extending and securing the infrastructure of the internet is absolutely necessary. In order to function as a network of global communication, the internet must be reliable and trustworthy, as formulated in the official statement of the multistakeholder NETmundial Initiative at its 2014 conference in São Paulo. Cooperating with the countries of the Global South is especially important when it comes to the goal of creating and extending internet infrastructure. The so-called digital divide between developed and developing countries has to be closed. Many people are still unable to access the internet, and this limits the opportunities for economic development in the countries concerned. Having open and stable access to the internet also gives citizens access to a wider range of political information, which could positively impact the development of democratic structures.

Internet security policy

In recent years, security concerns have increasingly shaped the regulation of the internet at the national and international levels. Hacker attacks on the servers of the German Bundestag and the IT infrastructure of DAX corporations, alongside the discussion surrounding the danger of espionage by the Chinese technology group Huawei as it pushes to expand 5G broadband coverage have driven—amongst other things—the national intelligence services to plan possible defense and counter-attack strategies (hackbacks).

The relevance of this topic is increasing, as is uncertainty about what sets of measures are best suited to meet the present challenges. For a 2019 study by the management consultancy Deloitte German executives and elected representatives from the Bundestag, the state parliaments and the EU Parliament were interviewed. It revealed that the manipulation of public opinion through targeted disinformation is now regarded as the most important cyber-risk—more so than online data fraud (70%), the theft of private data or information through cyberattacks (67%) or computer viruses and malware (65%).

In terms of regulation, the field is already well developed and includes national IT security laws as well as various directives and ordinances at the EU level. Within the UN, two parallel working groups have been established in the field of cybersecurity: the UN Group of Governmental Experts (UNGGE) initiated by the USA, and the Open-Ended Working Group (OEWG), proposed by Russia. Both are charged with examining how the principles of international law—e.g. the right to self-defense set out in Article 51 of the UN Charter—can also be applied to the internet. While many of the grim scenarios of deadly "cyberwars" have remained mere fiction, most experts assume that conflicts carried out over the internet between states, as well as between states and non-state political groups, will continue to increase in the coming years.

Photo: Cayambe / CC-BY-SA-3.0

Human and civil rights on the net

More recently, the topic of human and civil rights on the internet has come to the forefront as another field of internet governance. The debate on this question was catalyzed by the revelations made by NSA whistleblower Edward Snowden in the summer of 2013, which alerted the international public to surveillance activities carried out by intelligence agencies via the internet. The classified documents brought to light by Snowden made clear how extensive the online surveillance of citizens carried out by intelligence agencies has now become. The right to privacy is the right not to be subjected to arbitrary or permanent online surveillance by governments or economic actors. This right has especially received support from the EU's General Data Protection Regulation of 2018. In addition, there are other human rights and civil rights dimensions to internet governance. These rights include in particular freedom of opinion and expression, freedom of assembly and association and freedom of information. All of these civil liberties are exposed to special risks on the internet, especially in those countries with autocratic or non-democratic regimes.

The right to access the internet as well as the corresponding human right of development must be guaranteed, since the internet plays a vital role in the economic and social development of countries and societies. Like no other technology before, it has the potential to help people work their way out of poverty, and it must be allowed to be utilized as such by all.

Legal developments

The development of laws relating to the internet can be viewed as an encompassing field covering all the aspects of internet governance mentioned so far. While most experts agree that almost all the rules created for the offline world can claim to extend to the internet as well, the technical makeup of the internet creates certain peculiarities that render a simple translation of these norms difficult.

Therefore, it seems necessary to create new or adjusted rules, at least in certain cases.

Many observers doubt that in the near future the states will succeed in creating an international treaty regime that comprehensively regulates all legal relationships in the network for all participants and stakeholders. Previous concrete proposals for treaties, which have been submitted in particular by the Russian Federation and the People's Republic of China, have proved to be incompatible with the aforementioned civil liberties and have therefore been in conflict with existing international law rules. They were therefore rejected by the majority of the international community. Nevertheless, the objective of shaping internet regulation in accordance with international law should not be abandoned. A corresponding development can take place on the one hand through the emergence of customary law, i.e. without the agreement of international agreements. The rules thus created are equivalent international law. On the other hand, it cannot be ruled out that political sub-areas of internet regulation may be legally shaped by treaties between states. The successful conclusion of the Budapest Convention against Cybercrime, for example, has already shown that such international conventions are within the realm of the possible, at least for specific fields of the internet.

Of course, norms under international law are in any case only one way of advancing legal developments in the field of internet regulation (see also the FES publication *Völkerrecht in Zeiten des Netzes* [International Law in the Age of the Internet]). The different approaches are described in detail in the next section.

Approaches to, and possibilities of, internet governance

All countries and other participants in internet governance agree that the internet as a global communications structure is in need of regulation. However, how this is to happen, and who will preside over it, are questions for which there are no clear answers. In the following text, different approaches to internet governance are presented with the help of comparative conceptual pairings. There can be overlap between some of the pairs: for instance, the multistakeholder model is a bottom-up version of regulation that usually operates according to transnational mechanisms and leads to the creation of soft law. However, these concepts are not perfectly equivalent. Hence, it is useful to describe them separately, in order to better understand different approaches to internet governance.

Intergovernmental versus multistakeholder models

The two basic approaches to internet governance are the intergovernmental level, on the one hand, and the multistakeholder approach on the other.

Intergovernmental governance

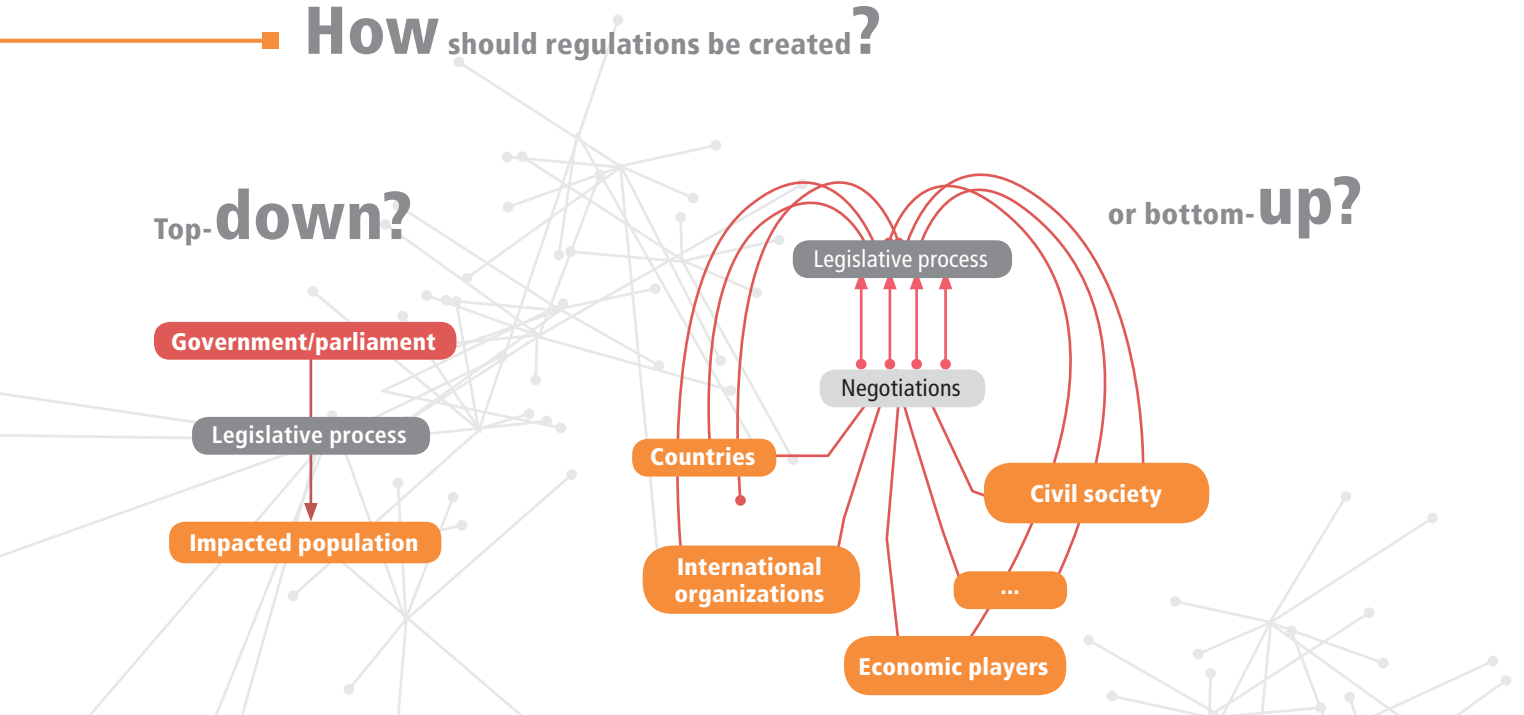
Intergovernmental governance consists of regulations created between specific countries or their respective governments. This is the traditional approach of international politics: national representatives meet at conferences or summits and engage in debates on the issues posed by a specific policy field, then they suggest solutions and negotiate how these suggestions can be cast as laws and regulations. Most of the international treaties currently in effect came into existence in this way, for instance, the Charter of the United Nations, the Law of the Sea Convention, and the Geneva Convention on Refugees. Resolutions of the UN General Assembly and the Security Council are also passed in this way. Virtually all preeminent international organizations, such as the Council of Europe, the African Union, and the World Trade Organization, operate similarly. The fundamental modus operandi of the European Union also follows the same pattern. This model gives the countries involved full control over both the process and the results of drafting regulations. With regard to internet governance, the primary example of the intergovernmental model would be the International Telecommunication Union.

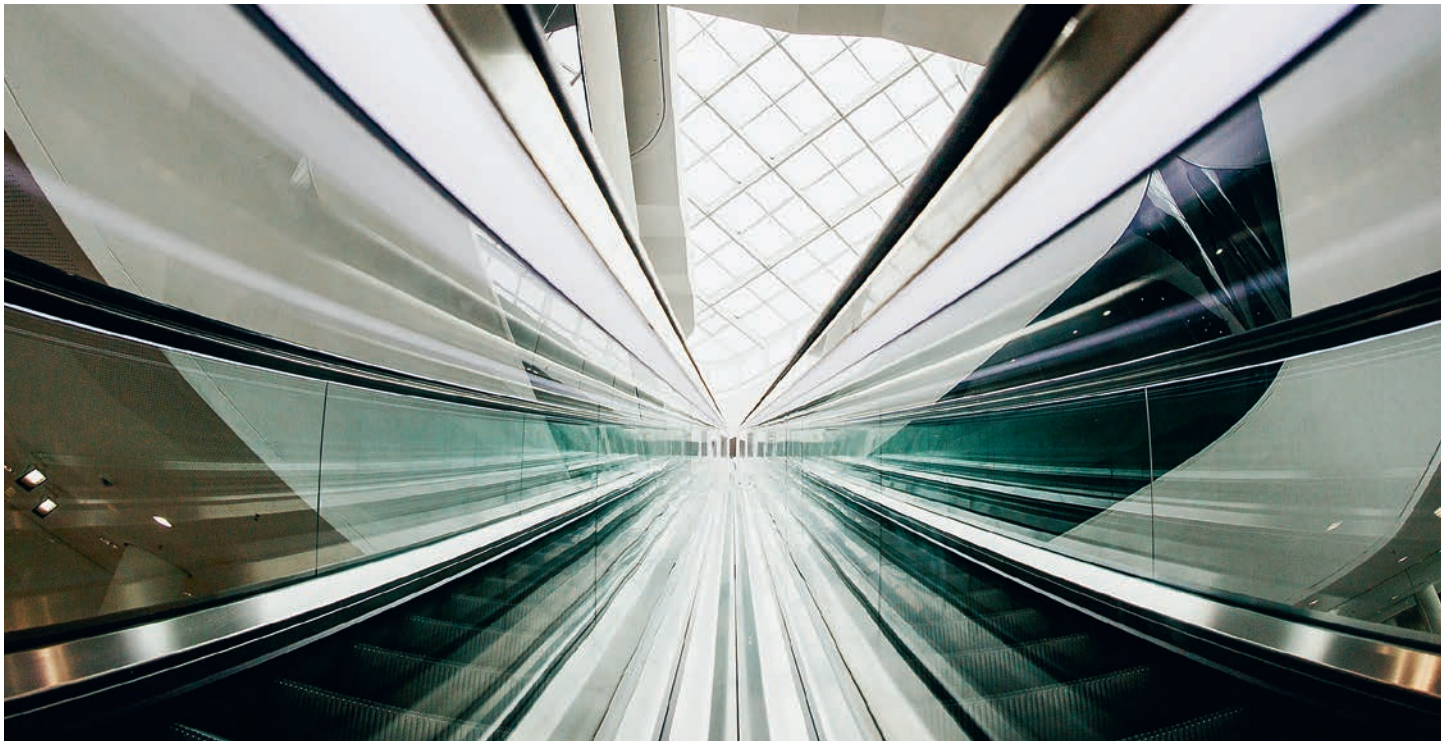
The multistakeholder model: involving everyone concerned

The multistakeholder model is relatively new compared to the more traditional intergovernmental approach. It attempts to involve all players that are impacted by an issue or policy as equal participants in the process of decision-making. Who the relevant stakeholders are depends on the field of policy in question. In the area of internet governance, they are the governments of the world's countries, private businesses engaged with the internet, representatives of civil society, NGOs, and international organizations. The multistakeholder model was first suggested by the Working Group on Internet Governance as a result of the first part of the World Summit on the Information Society in Geneva in 2003. It was designed as a compromise between exclusive governance by private businesses on the one hand, and exclusive governance by national governments on the other. Today this approach continues to be pursued at ICANN as well as at the Internet Governance Forum.

An ongoing dispute

Although leaving global internet governance solely in the hands of private businesses is no longer considered a serious option today, not least because of the skewed economic dominance of American IT companies, there is considerable disagreement regarding the question as to which of the two above-mentioned approaches to internet governance is preferable. While Western nations in particular have emphatically endorsed the multistakeholder model, a group of countries including China, India, Russia, Iran, and Saudi-Arabia have demanded extending the mandate of the ITU to the whole of internet governance. This suggestion was last made at the ITU Conference in Busan in 2014. The countries mentioned above defend the view that an international organization operating on the intergovernmental model is best equipped to protect their interests. However, the voting procedure at the ITU worries the representatives of Western nations, since, with relative ease, non-democratic governments can use their votes to block progressive





regulations conducive to their citizens' exercise of civil liberties on the internet.

However, it is not only authoritarian regimes that have voiced concerns about the multistakeholder model. Many governments of countries in the Global South have remarked that most of the stakeholders involved are from rich industrial nations. They point out that, for instance, anyone unable to raise the funds necessary to attend the relevant events would not be sufficiently involved in the multistakeholder process. Thus, decisions affecting all users of the internet might be taken without the required representation of poorer countries, which would put them at a disadvantage.

Top-down governance

The two approaches just presented are closely connected to another pair of concepts: the top-down and the bottom-up approaches to creating regulations. "Top-down" refers to decision-making processes that are carried out by an entity invested with higher authority. The standard example of such processes in the realm of national politics are laws passed by the legislative powers; in Germany, these are the Bundestag and the Bundesrat. The federal powers have indeed received their legislative mandate from the "bottom," i.e. from the citizens via periodical elections. However, the actual process of drafting legislation takes place in highly formalized processes on the governmental level. The laws passed in this way then impact the "bottom"—the citizens not directly involved in creating the actual legislation. This manner of passing binding legislation is the hallmark of representative democracies. In the area of internet governance, it is applied wherever countries themselves are the sole agents in a process of decision-making. This is the case predominantly in the intergovernmental forums and international organizations in which norms are created that oblige and bind the countries involved and, hence, their citizens through a "top- down" effect. In the field of internet governance, a typical example would again be the International Telecommunication Union.

The multistakeholder model: a classic "bottom-up" approach

In contrast to the model just described, the multistakeholder model is characterized by a "bottom-up" process. The stakeholders participating in the decision-making processes of the multistakeholder model act as equals. With regard to internet governance, this means that representatives of civil society or the economy can also exert a direct influence on the outcome of negotiations, instead of first conferring a mandate on democratically elected representatives. The advantage of this grassroots version of democracy is that, ideally, those who are impacted by a decision get to have their own voice in the process of its adaptation. This approach has been criticized as well, however, for possibly granting economic players or other powerful

entities a disproportionate influence—a danger, it is claimed, which can theoretically be minimized under the aegis of representative democracy. Furthermore, according to this point of view, the body of law that results from "bottom-up" processes tends to be fragmented and occasionally even contradictory.

Multilateral or bilateral?

Another set of concepts, closely connected to those already mentioned, which can serve to differentiate between different ways of developing regulations in the field of internet governance consists of "multilateral" or "bilateral" processes on the one hand, and "transnational" processes on the other.

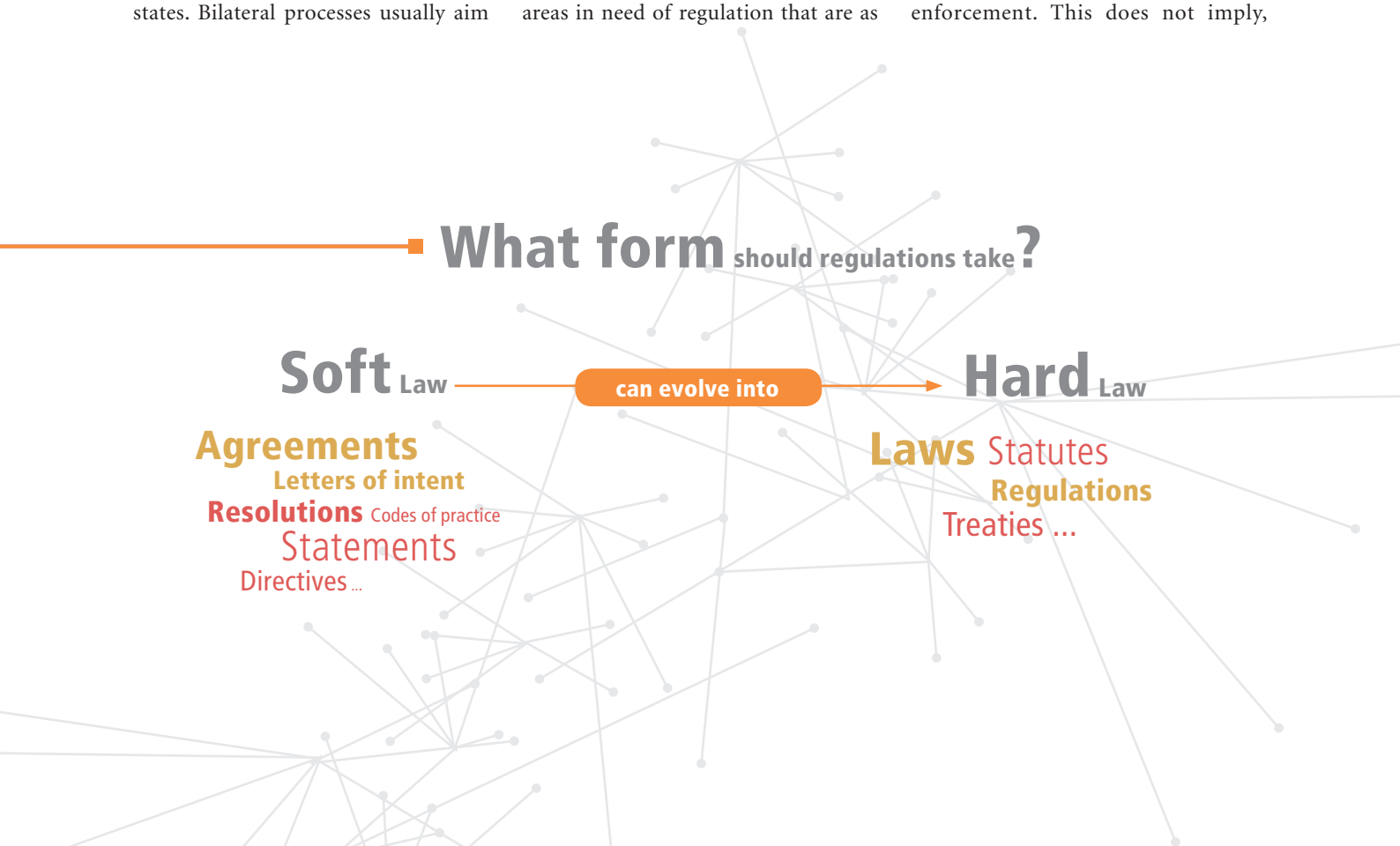
Decision-making processes are called multilateral or bilateral if they are conducted between governments in an international context. This can occur in a group of several countries organized at international conferences or within international organizations, or it can take place simply between two states. Bilateral processes usually aim to conclude a bilateral agreement. Due to the global structure of the internet, bilateral agreements concerning internet governance—apart from, say, questions of extending the infrastructure in regions near the border—are rare. The crucial arrangements for the issues not addressed by the scope of bilateral agreements are instead more aptly established in multilateral forums. The ITU again serves as a useful example.

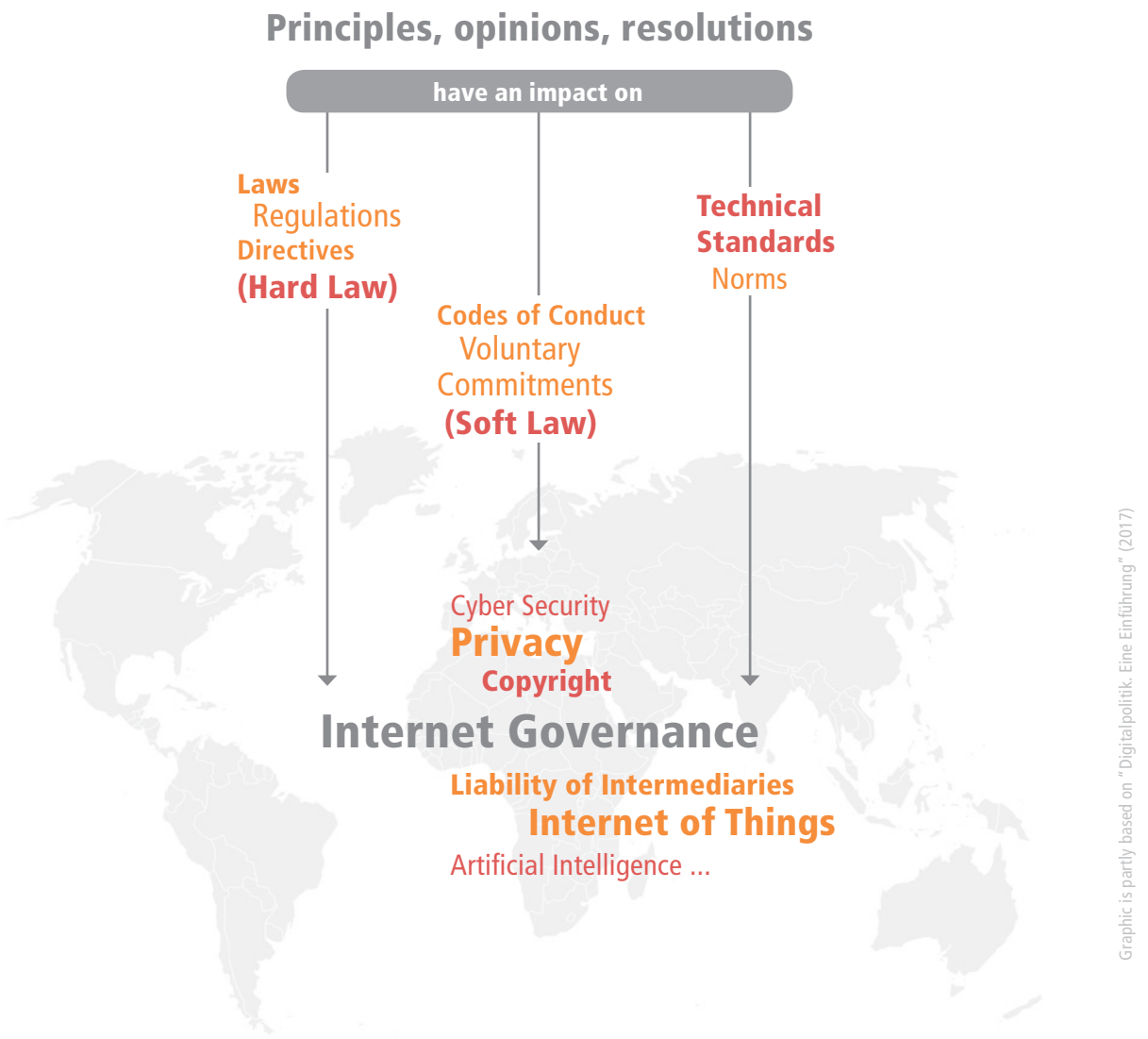
Transnational: beyond rather than between nations

In contrast, processes that do not take place between states but rather on a supranational level are called transnational. Transnational processes transcend national borders without national governments having exclusive control of them. Again, in this case, it is a matter of involving representatives of civil society in the decision-making process. The multistakeholder models at ICANN and IGF are paradigmatic examples of transnational mechanisms in internet governance. There are few areas in need of regulation that are as suited to the transnational approach as the internet, given that its structure is inherently transnational. Of course, national borders do play a role on the net, for example in the geoblocking of territorially licensed streaming content. However, many of the basic structures of the internet are designed transnationally, a feature that renders purely national solutions to its governance frequently inadequate.

Hard law vs. soft law

Finally, regulations in the field of internet administration can fall into the categories of either "hard law" or "soft law." "Hard law" designates those norms that can be identified as actual, genuine law, i.e. norms that force anyone subject to them to perform, or refrain from, certain actions. Hard law can be enforced through different means. A verdict handed down in a court of law is the obvious example, but by no means the only one. When it comes to international law, especially, there is often no specific legal authority that is responsible for enforcement. This does not imply,





Graphic is partly based on "Digitalpolitik. Eine Einführung" (2017)

however, that such regulations do not constitute hard law. Violations of such norms can be sanctioned in other ways, for instance by a resolution of the UN Security Council.

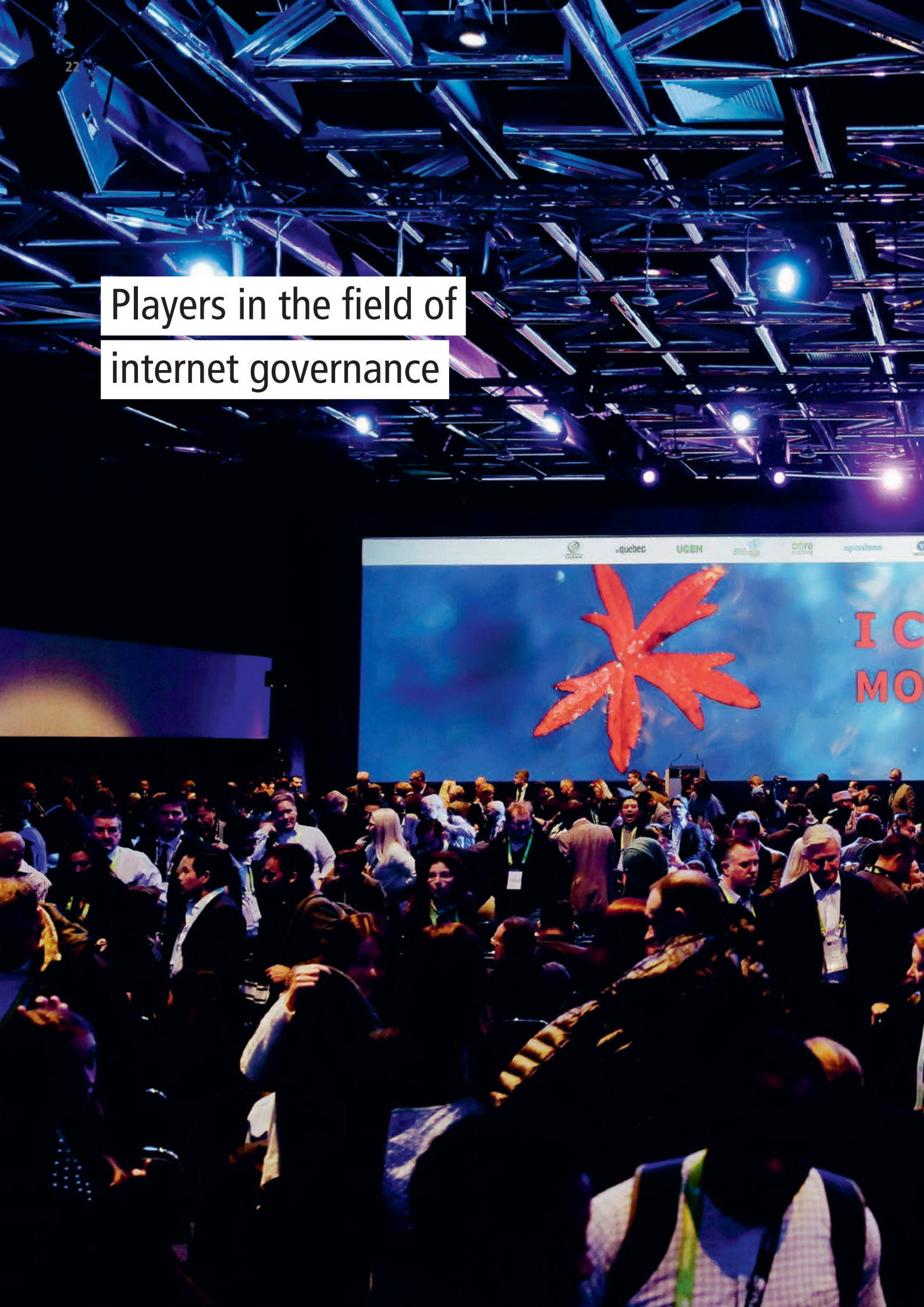
To govern the internet effectively, a large number of treaties, laws, and other regulations in the form of hard law are necessary. An example of an international treaty concerning internet governance would be the above-mentioned Budapest Convention on Cybercrime, which was created by the Council of Europe in 2001 and codifies a number of rules on combating cybercrime internationally. What is remarkable about this convention is that although it was created under the aegis of the Council of Europe, it is open in the sense that any country can ratify it even if it is not part of this international organization. As of today, the US, Canada, Japan, and Israel have joined the convention and have declared themselves bound by the regulations it contains.

On the other hand, "soft law" refers to agreements or statements that contain directives to anyone subject to the document but that cannot be enforced in a reliable way. On the international level soft law is very common. Many conferences or other meetings of national representatives do not result in binding resolutions or even international treaties, but rather in letters of intent or foundational agreements that express a consensus without encompassing any concrete, applicable law. Resolutions of the UN General Assembly fall into this category. In contrast to the resolutions of the Security Council, they are not enforceable.

The advantages of soft law

Especially in view of such fundamental differences in values, non-binding sets of rules are far more likely to be agreed upon at the transnational level. However, it should not be concluded from the non-binding nature of soft law that it has no regulatory impact. Once approved, such principles can often have a lasting effect on their target group: Following their establishment, the more parties that adhere to soft laws and that treat them as binding actually cause them to accumulate force and to become, in a way, hard laws.

Players in the field of internet governance



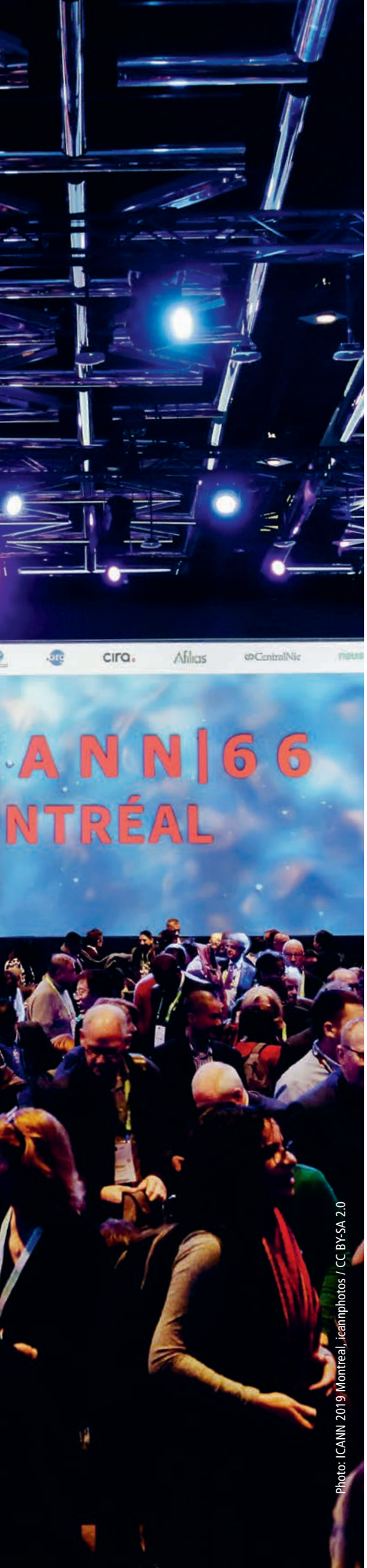


Photo: ICANN 2019 Montreal, icannphotos / CC BY-SA 2.0

There are many different players involved in the field of internet governance, as made clear in the preceding section. Especially with regard to the multistakeholder model, it is necessary to determine who the actual stakeholders in the internet are, so that their voices can be heard and they can be involved in the questions of internet governance. In what follows, the most important players in the multistakeholder model are described.

States

As a cross-border and global technical structure, the internet still requires governmental regulation in each country. Internet users are always subject to the laws and other regulations of the country they are in when they go online. Thus, every country initially creates its own laws of internet governance that are in effect within its own territory. Beyond that, the cross-border infrastructure of the internet, such as the transatlantic submarine cables carrying intercontinental data traffic, are jointly provided and maintained by the countries involved.

Proponents of the intergovernmental approach view countries, together with the international organizations that only exist by virtue of being founded and joined by member states, as solely responsible for internet governance. Advocates of the multistakeholder model, however, usually also regard it as self-evident that countries are important stakeholders. Thus, national representatives are usually present wherever internet governance is debated. This holds for the meetings of the Advisory Committee at ICANN as well as for conferences of the Internet Governance Forum (IGF).

Civil society

In Germany there are a number of interest groups, think tanks, and NGOs that are active in the field of internet governance and that can be classified as civil society stakeholders. They include, for example, the German chapter of the Internet Society, the Chaos Computer Club, and Digitale Gesellschaft (Digital Society). These non-profit organizations are concerned with general political questions involving the internet. They contribute to the debate by conducting studies or expert panels or by engaging in activism and public awareness campaigns. European Digital Rights (EDRi) is a European NGO umbrella organization in Brussels whose historical roots lie primarily in data protection and surveillance issues. In recent years, the national sections and volunteer communities of Wikimedia and the Open Knowledge Foundation have also repeatedly spoken out on political questions surrounding free knowledge and copyright law.

Increasing diversity

Access Now is an NGO with the ability and experience to run effective campaigns and which advocates freedom of expression, encryption technologies and net neutrality. It also works with telecommunications companies on transparency reporting. Another American NGO, the Electronic Frontier Foundation, also has a liaison office in Brussels and takes legal action against violations of consumer rights or internet users' privacy. This form of strategic litigation is also part of the repertoire of NGOs in Germany, such as the Gesellschaft für Freiheitsrechte / Society for Civil Rights.

In addition, some organizations should be mentioned that do not focus specifically on topics of the internet. For example, organizations such as Amnesty International or Human Rights Watch have committed

themselves to the task of monitoring, analyzing, and classifying whether human and civil rights are abided by on the net, and to sound the alarm if the situation worsens in any specific location. For some years now, the think tank Freedom House, based in Washington, D.C., has published a yearly report called "Freedom on the Net" that summarizes and evaluates the status of freedom on the internet across the world. Of course, initiatives from the Global South—such as the Centre for Internet & Society or IT for Change, both based in Bengaluru, India—also address issues of internet governance and the impact of technological innovations on democratic societies.

Of course, initiatives from the Global South—such as the Centre for Internet & Society or IT for Change, both based in Bengaluru, India—also address issues of internet governance and the impact of technological innovations on democratic societies.

Private sector actors

Besides participants from civil society, companies in the private economy and their related interest groups are undoubtedly stakeholders in the administration of the internet. After all, the infrastructure of the modern internet is for the most part (and in most countries) in private hands. This holds for internet service providers—in Germany, for example, Deutsche Telekom, 1&1 Drillisch, and Vodafone—as well as for internet giants such as Google, Facebook, and Yahoo. They all have an interest in participating in the issues of internet governance. Interest groups from the private sector—for example, Bitkom or eco in Germany—are also involved in the processes of internet regulation.

Private entities that are especially big or important and that, due to their economic position, have a major impact on the way the internet is used are sometimes themselves directly confronted with questions of internet governance. These are issues that they are spurred to solve either through their own initiative, or following interventions by the authorities in the form of court orders or antitrust resolutions. For example, in May 2014, the European Court of Justice enjoined Google to implement the so-called "right to be forgotten," i.e. to remove upon request any search results violating the right to privacy of an individual. Google then set up an Advisory Council in which two representatives of the management and eight external experts (including Wikipedia founder Jimmy Wales and former German Justice Minister Sabine Leutheusser-Schnarrenberger) were tasked with drawing up guidelines for data deletion and were to be consulted in difficult individual cases. In September 2019, the European Court of Justice clarified in a follow-up ruling that Google was only required to delete links EU-wide, rather that globally. Once again, the contradiction is revealed between territorially bound legal cultures and the broader aims of internet governance, namely to create universal rules and procedural security across the internet as a whole.

Photo: James Cridland. Crowd / CC BY 2.0

Regulated self-regulation

The adoption in Germany of the 2017 Network Enforcement Act (NetzDG) provoked a debate around the deletion of content. It was discussed whether the rigid deletion deadlines and steep fines for violations the Act imposes upon social platforms would motivate them to simply delete any content deemed problematic. Or whether they would, if in any doubt, undertake the

Three questions for Ioannis Kouvakas

Legal Officer at Privacy International in London

Photo: Private

"No one has time to read hundreds of consent forms every day"

Data abuse scandals are discussed in the media primarily in terms of large internet platforms. Is this focus justified in your opinion?

Ioannis Kouvakas: Yes and no. Generally speaking, public attention focuses on large companies such as Google, Facebook and Amazon, and perhaps on their Chinese competitors Tencent, Alibaba and Baidu—and rightly so. All these companies have become incredibly large and powerful in recent years. Security expert Bruce Schneier puts it well: "With every article written about Facebook's unpleasant stalking behavior, thousands of other companies breathe a collective sigh of relief that the spotlight is again being shone on Facebook and not on them. Facebook is unquestionably one of the biggest players in this field, but there are countless other companies that spy on and manipulate us for profit." This is one of the reasons that we filed legal complaints against data aggregators and so-called adtech companies in November 2018.

The revelations surrounding Cambridge Analytica have made the international public aware that elections are highly susceptible to influence by data analysis and microtargeting. Does the European General Data Protection Regulation (GDPR) offer an effective defense?

It is important to consider two aspects here. First, the so-called GDPR is nothing new. Yes, it brings a higher level of transparency, creates stronger guarantees for users' consent and control of their personal data and provides for steeper fines in case of violations. However, it is not the first data protection instrument. Data protection existed long before, and in Europe data protection laws were adopted decades ago. In other words, users' personal data is protected, not only because of the GDPR, but also because of a number of other legal instruments, many of which precede it.

Secondly, as with these other instruments, we should not forget that the GDPR is merely a law—a regulation, to be more precise. And although it aims to coordinate the protection of personal data, it is still up to the regulatory authorities to enforce and safeguard the rights of users. In other words, the law is nothing without its enforcement. The local data protection authorities must exercise their powers and condemn these data processing methods.

What can consumers do to defend their private spheres from a data capitalism that is constantly growing more technologically advanced?

We live in turbulent times—many people do not know whether and how to pay their rent, whether tomorrow they will still have a job or the right to stay where they are. Nobody has time to read hundreds of consent forms every day. It is currently extremely difficult for the individual to understand what is happening with their own data, but without strong data rights it is almost impossible to hold influential companies to account. Data rights do not only protect data. They also help compensate for the power imbalances between individuals, the state and the market—a relationship that is currently marked by extreme asymmetries.

Ioannis Kouvakas is a lawyer with Privacy International (PI) and works on a variety of projects at the interface of governmental and commercial surveillance and data misuse. His interests include national security, cyber security, privacy, technology and human rights. Before joining PI, he worked as a lawyer for NOYB (European Centre for Digital Rights) and for the European Fundamental Rights Agency (FRA) in Vienna.

Three questions for Dr. Matthias C. Kettemann

Lawyer and specialist on the normative order of the internet

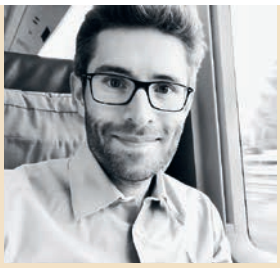


Photo: Private

"It's promising that things are moving in the direction of more cooperation"

Is our democratic public sphere even conceivable without so-called information intermediaries such as Facebook or Twitter?

Matthias C. Kettemann: There is no doubt that information intermediaries provide important spaces of communication where contributions can be made to public debate. Especially the perceptible presence—at least in interested circles—of certain politicians on social media enables a new intensity of interaction. Coordinated political activity, which also produces results offline—think of the #metoo and Fridays for Future movements—is strongly promoted by online communication.

However, social practices and the way people actually use the media are also decisive factors. The 2019 Reuters Institute Digital News Report for Germany, for example, has shown that even sections of the population with an affinity for the internet predominantly rely on other sources of information. As in the past, television remains the main news source for 45 percent of adult internet users in Germany. Only a small proportion of them only obtains information online.

How could one—below the threshold of legal regulation and beyond intransparent filtering practices—persuade information intermediaries to deal more responsibly with their curating role between facts, claims and recipients?

Many intermediaries prefer not to see themselves as curators of opinions; if they did, they would very quickly be in a position of editorial responsibility and could be held liable as soon as they became aware of any content on their platforms. Their algorithms and rules, which determine what content can be seen by whom and how, must be grounded in human rights and fundamental values. This can also be achieved through effective (externally regulated) self-regulatory mechanisms. The Council of Europe, for example, has provided a framework for this by adopting in 2018 the recommendations of its Committee of Ministers on the roles and responsibilities of internet intermediaries (MSI-NET), and setting important guidelines for the future design of rules for social networks. In particular, the protection of the integrity of elections and the fight against hate speech have led to a code of conduct within the EU for the self-regulation of large providers. Even if the absence here of clear self-control mechanisms and criteria to be met leaves much room for improvement, the direction in which these normative efforts are moving, i.e. of intervening through cooperative regulatory approaches in areas where binding legislation alone cannot achieve the desired goals, is in principle promising.

Right now, the discussion is focussed on containing disinformation and hate speech because we see them as a potential danger to democracy. Shouldn't the various actors responsible for internet governance pay more attention to setting standards for AI and decision-making algorithms?

There is no empirical evidence that disinformation and hate speech pose a threat to "democracy" as such. More dangerous are the shifts in socially agreed-upon frames of reference, the degradation of political culture, the seductiveness of anti-enlightenment behavior, and the wielding of dehumanizing language by politicians. We can't stop these developments merely by imposing tighter regulations on the use of algorithms by intermediaries. Although complex algorithms are not easily steered, at least some intermediaries have now begun to design algorithms that counteract the human tendency to engage with "borderline" content (which in turn makes it more likely that such content will be recommended to other users). As far as setting standards for algorithms is concerned, there currently exist so many declarations on the ethically sensitive design of algorithms that there is a danger of excessive standardization. Too many standards can also be harmful if it is not clear which regulations protect individual freedoms and promote social cohesion.

Dr. Matthias C. Kettemann, LL.M. (Harvard) is head of the research program "Regulatory Structures and Rule Formation in Digital Communication Spaces" at the Leibniz Institute for Media Research / Hans Bredow Institute (HBI), Hamburg, and deputy professor for public law, international law and human rights at the University of Heidelberg.

lengthy process of determining the degree to which human dignity has been violated. That is, weighing the importance of freedom of expression against that of preventing injury to someone's personal reputation.

This (corporate) approach is not only seen by net activists as a kind of de facto private jurisdiction. Many observers also fear a so-called "chilling effect" on free expression, as users increasingly refrain from making critical statements on the internet and in their haste restrict themselves in the full exercise of their basic rights.

Although the risk of such "over-blocking" could not be empirically verified at this phase, as the NetzDG is evaluated two years after coming into force, discussion has focussed on whether, if legally permissible content is deleted, a "pull-back procedure" should not also be in place to satisfy the claims of parties whose right to free expression is violated. Furthermore, merely deleting content constituting a criminal offense, such as death threats or hate speech, has been criticized as insufficient. As a result, the grand coalition government has announced that it will make further changes and clarifications to the Act, as well as introducing the requirement to report such content to to the authorities (status 11/2019).

A basic problem with enforcement here, however, is that claims to information regarding proven criminal conduct may amount to nothing, as the headquarters of Facebook and Co. are mostly located outside Europe, and they thus refer to the relevant legal cooperation agreements in those countries. Here, too, the grand coalition has announced that it will clarify the requirement for platforms to provide information. Furthermore, the EU Commission has announced that it will revise the European legal framework, thus far contained in the e-Commerce Directive, in the form of a new Digital Service Act (status 11/2019). It can therefore be assumed that increased platform liability for incitement or hate speech, alongside strengthened requirements for platforms to provide information to the authorities in such cases, will remain a regulatory point of conflict between the USA and the EU, also in the context of the deliberations on the European e-Evidence Directive and the American Cloud Act.

Another issue that will be under discussion during the evaluation of the NetzDG is the further development of the framework of so-called regulated self-regulation. The basic principle here, which is also applied in other policy areas, is that companies are legally required to self-regulate. In terms of internet governance, it can already be observed that commercial providers are developing binding codes of conduct for their platforms and, in case of infringements, take measures that are then regularly subjected to independent oversight. In this context, Mark Zuckerberg's public announcement in November 2018 that his company would be tightening its "Community Standards" and would establish an independent advisory board was welcomed as a step in the right direction, but also criticized as a further move towards the privatization of enforcement.

Inter- and supranational organisations

In addition to the organisations created for telecommunications in general or the internet in particular, which are arranged at international or transnational level, other international and supranational organisations also play a role in the regulation of the internet.

Besides the international or transnational organizations created for telecommunication in general, or the internet in particular, there are other inter- or supranational organizations that play a role in internet governance.

Photo: ITU, R.Farrell / CC BY-SA 2.0

The role of the United Nations

Since the beginning of the 21st century, when the momentous impact that the internet would have on civil, economic and political life worldwide had become apparent, the United Nations has attempted to take on a leading role in internet governance. Taking the initiative, it organized the World Summit on the Information Society (WSIS) in two parts—the first in Geneva in 2003, and the second in Tunis in 2005. After the first part of the summit was concluded, Kofi Annan, then Secretary General of the UN, appointed the Working Group on Internet Governance (WGIG), which was designed to identify and clarify fundamental questions in the field and develop suggestions for possible courses of action. The results of the Working Group were discussed in Tunis, and that second part of the summit led to the founding of the Internet Governance Forum (IGF), the purpose of which is to formalize and

Three questions for Moez Chakchouk

Deputy Director General of UNESCO

Photo: Nizarus / CC BY 2.0

"The internet is much more than infrastructure and applications"

How does UNESCO perceive of its role in terms of multilateral internet governance issues?

Moez Chakchouk: UNESCO acknowledges the potential of the internet for fostering sustainable human development and building inclusive knowledge societies, and also for enhancing the free flow of information and ideas throughout the world. UNESCO, together with ITU, has also launched the Broadband Commission for Digital Development. The purpose of the Commission is to define strategies for accelerating broadband rollout worldwide and examine applications that could see broadband networks improve the delivery of a huge range of social services, from healthcare to education, environmental management, safety and much more. UNESCO's approach to internet governance is based on its Internet Universality framework. Internet Universality is a concept and framework adopted by UNESCO in 2015 to summarize the organization's positions on the internet.

The concept recognizes that the internet is much more than infrastructure and applications, it is a network of economic and social interactions and relationships, which has the potential to enable human rights, empower individuals and communities, and facilitate sustainable development. The concept is based on four principles stressing that the internet should be human rights-based, open, accessible, and based on multistakeholder participation. These have been abbreviated as the R-O-A-M principles. Understanding the internet in this way helps to draw together different facets of internet development, concerned with technology and public policy, rights and development. Through the concept of Internet Universality, UNESCO highlights four separate but interdependent fields of internet policy and practice that are considered "key" in assessing a better internet environment; access to information and knowledge, freedom of expression, privacy, and ethical norms and behavior online.

For many observers, the World Summit on the Information Society (WSIS) in Tunis in 2005 provided the initial spark for deeper engagement with net policy issues. Apart from the IGF, don't we need more spaces for international discussion on urgent issues like data protection and free access to information?

One of the principles of the concept of Internet Universality relates to multistakeholder participation as an essential element in successfully building a people-centered, inclusive and development-oriented information society. UNESCO encourages the development of multistakeholder processes at the national, regional and international levels to discuss and collaborate on the expansion and diffusion of the internet. The International Day for Universal Access to Information is an important opportunity to discuss these issues, including awareness that the right to infor-

provide continuity to the discourse around internet governance. Within the United Nations, too, questions regarding the administration of the internet arise periodically. Here, special emphasis should given to "The Right to Privacy in the Digital Age," a resolution brought forward by Germany and Brazil at the General Assembly in December 2013. In response to the NSA scandal following revelations by the whistleblower Edward Snowden, the resolution established that the privacy of individuals on the internet is to be protected from arbitrary or other unjustified forms of government interference.

Efforts to strengthen multilateralism in the sphere of internet regulation have recently come to the fore within the UN. In the summer of 2019, the UN General Secretariat presented a report titled "The Age of Digital Interdependence," which summarized a year of work by an international panel of experts. In it, the UN emphasizes its unique ability and authority to bring together various stakeholders and jointly set the standards and build the frameworks that can ensure a just digital future for all. In support of this claim, the report puts forward recommendations for action and various models for how the multistakeholder model can be further developed (more on this in the final section). With its sub-organizations, the UN could indeed play a major role in monitoring compliance with the global sustainable development goals in digital production and in initiating other standard-setting processes, for example in the area of cyber security.

mation is essential for transparent and accountable governance and a prerequisite for public involvement in formulating social policies and other decision-making processes.

How do you personally experience the knowledge gap in terms of the technical infrastructure of the internet?

Infrastructure and technology development are essential elements in building knowledge societies. Inequalities of access to sources of information, content and infrastructure cast doubt on the global character of our information societies and, consequently, hamper their growth. There is a knowledge gap in terms of technical infrastructure; this is why UNESCO promotes the concept of media and information literacy, which includes competencies related to internet literacy. The Information for All Programme (IFAP) has been advocating for enhanced knowledge across a range of media and other information providers such as the internet. UNESCO's media and information literacy policy and strategy guidelines also advocate for basic information literacy training that targets upper primary school students and adults.

Moez Chakchouk is Deputy Director General of the United Nations Educational, Scientific and Cultural Organization (UNESCO) and Head of the Communications and Information Section, which is also responsible for internet management, general media development and the development of artificial intelligence. The internationally renowned ICT expert is an engineer, studied in Paris and Tunis and was a top civil servant in the Tunisian public sector. Previously, he was Chairman and CEO of Tunisian Post.

OECD and WTO

Further international organizations to be mentioned in this context are the Organization for Economic Co-operation and Development (OECD), and the World Trade Organization (WTO). Under the aegis of the WTO, which was founded in 1995, the Information Technology Agreement (ITA) was created, which regulates tariffs and trade barriers of virtually all trade in IT products worldwide. This can be classified indirectly as internet governance. The General Agreement on Trade in Services (GATS), also created by the WTO, includes the regulation of cross-border trade in the area of telecommunications.

The OECD has also addressed internet governance issues on a number of occasions. Already in 2010, the OECD report "The Economic and Social Role of Internet Intermediaries" provided groundbreaking definitions and assessments of today's ubiquitous digital "platform capitalism." At the

organization's ministerial conference in Paris in June 2019, digital competition policy was at the top of the agenda.

The EU

The European Union is active in various areas of the field of internet governance, in particular through its direct regulatory activity in the European domestic market. An important example of this is the so-called Digital Agenda for Europe, authored by the European Commission in 2010, which created the framework for a digital domestic market in Europe. In recent years, the EU Commission has notably stepped up its efforts to intervene in regulatory policy and to harmonize procedures. This process has been marked by a balancing of the perspective represented by the member states in the Council, which is oriented towards economic goals, with the more consumer-oriented and participatory view represented by the Parliament. The most important legal instruments in this area in recent years have been the General Data Protection Regulation (2018), the Directive on Copyright in the Digital Single Market (2019) and the ePrivacy Regulation, which is still under discussion. By conferring authority for digital policy to the Competition Commissioner Margrethe Vestager (Denmark), the new Commission, led by President Ursula von der Leyen (Germany), has sent a clear signal that further regulatory steps will follow—e.g. in drafting the planned Digital Services Act or on the question of a digital tax—which are likely to generate some internal controversy.

International Telecommunication Union (ITU)

The International Telecommunication Union, which was founded in 1865 as the International Telegraph Union, became a specialized agency of the UN in 1947 and is based in Geneva. Its responsibilities primarily encompass the technical aspects of telecommuni-

Photo: ITU, D. Woldu / CC BY-SA 2.0

Three questions for Laura-Kristine Krause

Co-Chairwoman of D64 and Managing Director of More in Common

Photo: Private

"I see the greatest leverage at the European level"

Is there a specifically social-democratic focus on certain aspects of internet regulation?

Laura-Kristine Krause: Freedom, justice, solidarity—these are all values that must be upheld, especially in the age of the internet. A social-democratic perspective on digitization is thus very important, but also means that we must renegotiate what it means to preserve these values in practice. A digitized world often calls for new formulas and approaches in order to realize these old (but highly relevant) values.
This applies, for example, to the challenges of social coexistence in a digital society and the ways that we deal with digital capitalism, but especially to the digitized world of work: digitization allows people greater flexibility and autonomy in earning a living by, for example, allowing solo freelance work to become something of a normality. At first glance this may seem like a step backwards in light of the achievements of classic social democracy. However, the task of social democracy is to ensure that social standards are maintained without at the same time standing in the way of social change.

In your opinion, what should Germany do to ensure the widest possible range of participation in discussions on the future of the internet?

First and foremost, the future of the internet should be seen as a natural aspect of broader policy debates. Far too often, digital issues are discussed "separately" among digital policy specialists, rather than being integrated into future-oriented debates in other policy areas. In order to maximize people's participation in these discussions, it is also important that future debates on digitization are not constructed as technical-abstract discussions, which could potentially have a deterrent effect, but as what they really are: important contributions to our shared future, to the future of our society and to our future prosperity.

In view of the global nature of the internet, do you believe in the effectiveness of national laws that can, at least potentially, spur international competition for the best solutions?

Of course, it is important to pursue regulatory approaches to digital policy issues at the national level, but this must always be done with a focus on what makes sense and what actually has the best chance of achieving the envisaged goals. However, in terms of driving competition for the best solutions, I see the greatest potential leverage not at the national level, but at the European level: Because of the size of the European common market, this is where the potential exists to actually bring about impactful change and steer things in the right direction. The best example of this is the General Data Protection Regulation, which is little appreciated in Germany, but which, because of its broad scope, has set a regulatory standard that extends far beyond the borders of the EU. Numerous actors in the USA, for example, are now adhering to its provisions. However, for the EU to strengthen and expand its role as a "pioneer regulator," national regulators would need to participate more constructively in digital policy debates at EU level. As the adoption of the EU copyright directive has shown, there is a lot of room for improvement here—especially when it comes to a healthy competition for the best solutions.

Laura-Kristine Krause is co-chair of the SPD-affiliated think tank D64—Center for Digital Progress. She is also an honorary member of the Rhineland-Palatinate State Council for Digital Development and Culture and of the Digitalbeirat des Landes Brandenburg (Brandenburg Digital Advisory Council). Krause is the founding managing director of More in Common Germany. Previously, she was program director of the think tank Das Progressive Zentrum and senior associate at a strategy consulting firm. Her previous professional positions included work in the election campaign team of Hillary Clinton.

cation. This includes coordinating the assignment of radio frequencies on a global scale, instituting international cooperation with regard to the orbits of telecommunication satellites, developing global technical standards, and coordinating collaboration with countries of the Global South with regard to the extension of their communication technology infrastructure. Chinese-born Houlin Zhao has been the head of this organization since 2015.

The ITU is open to all countries and currently has 193 members. Even though private companies and organizations such as internet providers, manufacturers of technical appliances, and research organizations may also become members, the ITU follows the intergovernmental model rather than the multistakeholder one. Any members that are not countries hold only an advisory and observer status, and do not have the right to vote. Elections follow majority rule. The supreme body of the ITU is the Plenipotentiary Conference, which convenes every four years.

Three questions for Prof. em. Wolfgang Kleinwächter

German doyen in the field of internet governance

Photo: re:publica / CC BY-SA 2.0

"There is no alternative to a collective approach"

To what extent does the "digital authoritarianism" of countries such as China or Russia, clash with the UN's goal of creating new architectures for global digital collaboration?

Wolfgang Kleinwächter: The new complexity of internet governance reflects a broader political status quo at the end of this decade: Digital neo-nationalism is on the rise. In 2018 Freedom House dedicated its annual Freedom on the Net report to "The Rise of Digital Authoritarianism." More and more governments view global internet-related policy issues primarily through a national lens. They want to control the flow of data which crosses their borders. They fear that borderless communication will undermine national security, their domestic digital economies or local cultures. Key words are "cyber sovereignty," "national Internet segments" or "my country first." The aim is to re-introduce the borders which the information revolution had removed when TCP/IP and DNS based networks embraced the entire globe.

Many governments do not believe anymore in global solutions to the fight against cyberterrorism, cross-border cybercrime or digital monopoly. They prefer unilateral actions within their own jurisdictions. Russia has built its own internet root, China filters harmful content. Iran, Saudi-Arabia and India have introduced strong data localization laws. The US excludes Huawei from building 5G networks. France opts for a digital tax. Germany pushes Facebook to block fake news and hate speech. And governments in many developing countries simply block all internet access if something is happening which they do not like. Twenty two African states—out of 51—have disrupted connectivity over the past five years.

Does that mean we're going backwards and reintroducing barriers that were actually eliminated by the digital revolution?

A fragmented internet would reduce the overall utility of the global network, lead to instability in cyberspace, hamper innovation and economic growth, promote national protectionism, and encourage local censorship and surveillance. It would open doors for new forms of confrontation between "national Internet segments," including "network wars" fought with a new generation of cyberweapons. Today, some governments see the global internet less as a win-win-situation but more as a zero-sum game, with winners and losers. They believe that they can gain national political stability (and strengthen local power) if they regulate the internet by limiting related economic and social activities within their territory. But there is a flip side to this approach. The re-introduction of national borders into cyberspace does not actually create more security. It leads to an illusion of control, but does not correspond to the realities of the information age. As with environmental issues, unilateral action does not settle the global problems of mankind.

Since the beginning of the century, the ITU has attempted to gain a foothold in the field of internet governance. It was one of four UN agencies that organized the 2003 and 2005 World Summit on the Information Society. Nevertheless, so far the role of the ITU has mainly been limited to technical and infrastructural questions.

The ITU as the main agency of internet governance?

On the initiative of Russia, China, and India, concrete suggestions for changes to the founding treaty of the ITU were first proposed at the World Conference on International Telecommunications in Dubai in 2012. These included extending the mandate of the organization to include the functions previously performed by ICANN. The countries mentioned above expressed as their main argument the concern that the US would wield too much of an influence over the private organization, which is based in California. The draft of the new treaty was criticized severely not only by the Western countries and the European Parliament but also by representatives of the private sector. Google, for instance, published a statement condemning the suggestions as an attack on a free and open internet.

The above-mentioned countries again tried to achieve an extension of the responsibilities of the ITU at another ITU conference in Busan, South Korea in 2014, even trying to include topics such as the right to privacy and government surveillance. These plans were thwarted by Western nations, headed by the US, which responded to criticism by referring to the multistakeholder model that is to be implemented. At the ITU Conference 2018 in Dubai, its member states drew up a roadmap for 2020 to 2023 and discussed issues fundamental to digital competition such as market entry thresholds and merger controls.

At the IGF 2018 in Paris, French President Macron proclaimed the need for an "innovative multilateralism" in matters of internet regulation. Would this not demand even greater involvement by non-state actors in the main international policy fora—such as the UN, WTO, G20?

The UN High Level Panel on Digital Cooperation has spoken of "The Age of Digital Interdependence." Interdependence means that no country can continue to exist in isolation. It also means that solutions can only be found through enhanced cooperation among all stakeholders, i.e. governments, business, civil society and the technical community. Furthermore, it means that solutions can only be found by understanding that cybersecurity, digital trade, human rights and technology are all interlinked. There is no alternative to a holistic and collective approach. Innovative multilateralism demands wisdom and courage, but above all political good will, which is a rarity in our time.

Digital unilateralism offers low hanging fruits, but these fruits are poisoned. Digital unilateralism can lead to the weaponization of cyberspace, digital trade wars and massive online violations of human rights. It can undermine stability in cyberspace, a space which is used by more than half of the world population. Cyberspace was created by people, but for future generations it will be part of a common heritage, of their natural ecosystem. One should have no doubt that instability in cyberspace is as dangerous as climate change.

Wolfgang Kleinwächter is Emeritus Professor of Internet Policy at the University of Aarhus. He is a member of the Global Commission on Stability in Cyberspace, has been a member of the ICANN Board (2013-2015) and Special Ambassador of the Net Mundial Initiative (2014-2016). He also advises numerous committees and institutions on internet governance and security, including the UN, the Internet Governance Forum (IGF) and the EU.

Internet Corporation for Assigned Names and Numbers (ICANN)

ICANN was founded in 1998 on the initiative of the US Department of Commerce. Its headquarters is in Los Angeles, California. It is a private non-profit organization that administrates the Domain Name System (DNS) of the internet on behalf of the Department of Commerce. The DNS is a global network of databases that records domain names and corresponding IP addresses. It has been called the telephone book of the internet.

Photo: Kranich, pixabay.com / CC0

ICANN is not subject to direct control by any government. It does not have any governmental authority either. Its regulations concerning the internet come into effect by way of civil law treaties made with other organizations, especially in countries other than the United States. As mentioned above, this organization is one of the prime examples of the multistakeholder model. Its central institution is the board of directors, which has 21 members, and which makes crucial decisions only after having negotiated with a committee composed of government representatives from 110 countries. Representatives from the private sector, the tech community, academia and civil society are also involved in the decision-making processes.

Compatibility with EU law?

Shortly after the General Data Protection Regulation came into force in May 2018, ICANN filed a lawsuit against a German domain registrar at the Bonn Regional Court. The question before the judges: Was the company required to collect complete administrative and technical contact information—so-called WHOIS data—for new domain registrations, as stipulated in principle by its ICANN accreditation? The court found that the company's more economical handling of data was sufficient to prevent misuse. However, the court did not comment on the question of whether the data transmission practices required by ICANN themselves constitute a breach of the GDPR. ICANN then announced that it would continue discussions with the European Commission and the European Data Protection Supervisor on the integrity of WHOIS services.

Internet Governance Forum (IGF)

The Internet Governance Forum has been called the paradigm of the multistakeholder model in the field of internet governance. Founded in 2006 as an outcome of the World Summit on the Information Society, convened in 2003 and 2005, the IGF constitutes the first continuous and globally-oriented forum for debates involving internet governance. Part of the motivation for the UN's founding of the IGF was to create a counterbalance to the US-based ICANN. In contrast to ICANN, however, the IGF does not have a mandate to pass binding resolutions.

The IGF meets yearly and invites representatives of governments, as well as the other stakeholders mentioned above, to participate in the debate surrounding internet regulation. In November 2019 the IGF convened for the first time in Germany.

The organizational structure of the IGF encompasses the Secretariat, which has offices in the UN headquarters in Geneva, and the Multistakeholder Advisory Group (MAG), which is responsible for preparing both the facilitation and the content of its yearly meetings. The MAG currently consists of 56 members and is composed of representatives of all stakeholders. It attempts to rotate about a third of representatives from its different stakeholder groups each year. In addition, there are currently 17 regional and sub-regional IGFs. The overall aim of these offshoots is to create additional spaces for dialogue in which various actors can discuss those internet issues most relevant to the needs of their respective communities. One such space is the European Dialogue on Internet Governance (EuroDIG), which attempts to bring together national perspectives while developing European models and positions on the internet.

Institutionalizing the Internet Governance Forum in Germany

Since the founding of the IGF, many regional and national forums have been established. The German branch of the IGF, the Internet Governance Forum Germany (IGF-D), has existed as a loose structure since 2008. It promotes an open process of discussion, as required by the multistakeholder model, and convenes a yearly conference that brings together national players in the field of internet governance. Similar to international forums, its job is to maintain and elaborate the dialogue on internet regulation, but on a national level.

Since the beginning of 2016, IGF-D has included an advisory committee and a secretariat. The advisory committee is composed of representatives from politics, science, the economy, and civil society. It advises IGF-D and promotes its work to the general public. The secretariat is based in the offices of Reporters Without Borders.

In what direction are developments pointing?

In its report "The Age of Digital Interdependence," the UN proposes three possible paths towards building a suitable architecture for global digital cooperation:

— The "IGF plus" model assumes that the involvement of more representatives from government and the private sector would produce more concrete results, provided the various strands of discussion were moderated appropriately. To this end, new bodies (Advisory Board, Trust Fund) and new functions could be established. A "cooperation accelerator" would have the task of maintaining the focus and intensity of cooperation across a large number of institutions, organizations and processes by identifying points of convergence between existing coalitions and questions around which new, preferably multidisciplinary groups, could be formed. A "policy incubator" would provide the currently missing link between the dialogue platforms, whose task is to identify regulatory gaps, and policy-making bodies by keeping up the momentum of discussion, even if unable to make legally binding decisions itself.

— A "Distributed Co-Governance Architecture" approach would aim to use the proven model of horizontal networks to decouple the three stages of identifying regulatory gaps, implementing regulation, and enforcing regulation from one another and deal with them each according to a division of labour. Self-governing, open "digital cooperation networks" would have the task of designing digital standards. "Network support platforms" would stabilize participation in these networks and support them in working efficiently, but would not interfere with the content of their work. In contrast, a "network of networks" would have a coordinating role in organizing forums for exchange at regular intervals. Once standards were agreed upon, the relevant government authorities could use these as blueprints while defining appropriate enforcement mechanisms.

— The "Digital Commons Architecture" model is based on the commons movement, which aims to protect and maintain common goods according to certain principles. This perspective is also increasingly being taken into account in debates on data ethics or AI. Procedurally, these debates would be channeled through "multistakeholder tracks" and annual meetings, supported by a UN secretariat. This approach does not define technical solutions, but merely proposes models and standards for responsibilities. It could also promote the collection and discussion of global solutions for the implementation of existing standards in specific areas.

These three models are all built on the multistakeholder principle as a basic template and could be flexibly combined with each other. It will be interesting to see whether and how these proposals find expression in the practical design of internet governance.

The UN proposes three possible paths towards building a suitable architecture for global digital cooperation:

IGF plus

Distributed Co-Governance-Architecture

Digital Commons

Discussion and outlook

Photo: Gregor Fischer, re:publica / CC BY 2.0

Digital innovations are changing life in our society, and the pace of this change is constantly accelerating. New technologies from the field of machine learning and AI or blockchain applications are putting existing regulatory paradigms to the test. Many of these applications quickly migrate to other sectors, ranging from agriculture, banking, climate protection, digital education, e-government and e-health to intelligent transport and energy management systems.

Solutions to social challenges are rarely found in self-contained silos of knowledge. Thinking about the digital society must therefore be international, interdisciplinary and internet-based. At the same time, international politics has created high-profile events, such as the annual meetings in Davos, to draw the broad lines of economic policy and competitive conditions in the field of digital value creation. Here it becomes clear: With regard to the internet, we no longer find ourselves in a regulatory desert, but in an increasingly mapped area in which many claims have already been staked.

Internet governance in all its facets has always been a contested terrain. For years, the debate revolved around the question of whether international internet policy should be regulated by multistakeholder agreements or multilateral treaties. The high output of national legislation on cyber security, surveillance, content filtering or the taxation of data-driven businesses has led to new controversies. In order to deal with these lines of conflict, we need actors who trust each other and discuss solutions with each other. And that's exactly where it hooks right now.

An old debate, rekindled

The USA, which for decades has been a pioneer of freedom on the internet, has translated its "America first" approach into a national cyber strategy under the Trump administration. This tough stance resembles those of China and Russia, which oppose the "innovative multilateralism" called for by Emmanuel Macron at the IGF 2018 with neo-nationalist unilateralism. "This global debate," writes Wolfgang Kleinwächter, "began in the early 1990s. In the first few years, it revolved around the management of critical internet resources. But since the Tunis Agenda of 2005, which introduced the multistakeholder approach, the discussion has extended to all areas of global governance: from security to trade to human rights. 20 years ago, the Internet was a technical problem with political implications. Now it is a political issue with a technical component."

From the European perspective, the Snowden case constituted a kind of "reality shock" (Sascha Lobo), in any case a mental caesura. With the NSA revelations it definitively became clear, if it hadn't already, that the free and open internet is a structure that must always be fought for anew. The first generation to grow up with and on the

Thinking about the digital society must be international, interdisciplinary and internet-based.

internet has been confronted with the realization that the guiding ideals of informational self-determination and the absence of censorship, repression and surveillance are not givens. And so the youth takes action, at times with completely analog means: Hundreds of thousands of young Europeans took to the streets to protest Article 17 of the EU Copyright Directive or ACTA because they saw their online freedom threatened. One could conclude that this is indeed a fruitful time for internet governance.

Loss of control and political courage

The flip side of freedom is the fear of losing control. And this fear is no longer restricted to industries whose business models have become obsolete in the course of digitization. Even those who saw in the internet a second, additional layer to the democratic public sphere are now concerned about the accumulation of disinformation campaigns on social platforms. Traditional journalism, with its principles of editorial responsibility, now must find new ways to research and share information if it hopes to survive these changing times.

All actors in internet regulation are called upon to try to square the circle: reconcile freedom of expression and information with the interdiction of criminal content or false claims. In the medium term, this complex challenge could be a litmus test for the newly awakened digital public sphere with its interactive feedback channels, relentless acceleration and chances for participation.

It is also important to preserve the diversity of the internet's ecosystem. The current market dominance of the US "Gang of Four" (Google, Amazon, Facebook, Apple) and the old behemoth Microsoft conceals the fact that, away from these great "landmasses" of the internet there are many other small islands whose founding idea had nothing to do with aggregating and commercially exploiting data. It is actually a miracle that the online encyclopedia Wikipedia, which is financed by donations, is still among the top ten most visited websites worldwide.

Expanding the multistakeholder model?

We must strenuously object to the present tendencies of authoritarian regimes like China's, which has created a "Great Firewall" to shelter itself from any uncomfortable content. Above all, however, it is important to keep the underlying structure of the internet stable and to prevent its fragmentation into a so-called "splinternet," divided by the geographical borders of various countries and regulated only by local laws. This outcome would undoubtedly spell the end of the original, universal idea behind the internet.

The forces for an open and free internet are still alive and kicking. This can be seen from the growth of civil society actors and the efforts in the private sector (including political and corporate foundations) to bring about new procedures of participation and greater transparency. Even the UN, whose decision-making power in the Security Council has been paralyzed for years, is calling for new initiatives. According to the UN report "The Age of Digital Interdependence:"

"Effective digital cooperation requires that multilateralism, despite current strains, be strengthened. It also requires that multilateralism be complemented by multi-stakeholderism-cooperation that involves not only governments but a far more diverse spectrum of other stakeholders such as civil society, academics, technologists and the private sector. We need to bring far more diverse voices to the table, particularly from developing countries and traditionally marginalized groups, such as women, youth, indigenous people, rural populations and older people."

There are therefore good reasons for maintaining the multistakeholder model both at ICANN and in discussion forums such as the IGF. Only this approach can ensure that the voices of the entire internet community are heard. Transnational decision-making processes and bottom-up regulation mechanisms actually correspond to the diversified stakeholder structure of the internet, and do better justice to the actual web of interests at stake than multilateral standards imposed top-down by governments alone.

Glossary

Access Provider: Company that allows customers access to the internet.

ACTA (Anti-Counterfeiting Trade Agreement): Planned multilateral trade agreement that would have existed as international law and which, among other things, would have set international standards in the fight against product piracy and copyright infringements. After viral online campaigns and mass demonstrations in numerous European cities, the EU Parliament rejected ACTA by a considerable majority in July 2012.

Advocacy: Activity carried out by a person or group that aims to indirectly influence decisions in political, economic and social systems and institutions, as opposed to direct lobbying, by using facts and messages to educate the public. Advocacy instruments used by NGOs or associations include media campaigns, awards, public appearances or research results.

African Union (AU): International organization based in Addis Ababa, Ethiopia, and Johannesburg, South Africa, which promotes the cooperation of the nations of Africa. All nations of the continent except Morocco are members.

Browser: Computer program allowing users to view pages of the World Wide Web on their devices. Web browsers serve as user interfaces for most web applications. Well-known browsers include Google Chrome, Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari.

Confidence Building: A term from international politics that designates measures intended to reduce tensions between countries that might otherwise pose a threat of political crises or even armed conflict.

Council of Europe: An international organization founded in 1949 which has 47 European nations as its members. It is based in Strasbourg, France. Its purpose is to coordinate the regional politics of the nations of Europe. Its foundational center lies in the European Convention on Human Rights, passed by the Council of Europe, and the European Court of Human Rights.

Cyberattack: A general term encompassing all harmful actions carried out in cyberspace by means of information technology. The motives of cybercrime can be criminal or political in nature.

Cybercrime or computer-related crime: Refers to crimes committed against, or by means of, the infrastructure of information and communications technology. The tools used to commit the crime are thus a network as well as one or more computers connected to it.

Cyber security: This term encompasses any measures intended to protect computers, networks, and other parts of the infrastructure of information and communications technology from attacks.

Cyberspace: This term is often used synonymously with the internet. However, it is to be understood more broadly as the totality of virtual space in which communication between computers or networks of computers takes place.

Digital Divide: This is a term from political science that designates an economic or social inequality of access to modern information and communications technology. It can refer to the state of affairs within a particular country or between different countries on an international level.

Domain name: The part of a web address (e.g. www.fes.de) identifying it as belonging to a specific domain. Domains are administrative units in a network that can exist on different levels. The example given shows that the website of the Friedrich Ebert Foundation belongs to the top-level domain ".de," i.e. the highest level encompassing German websites.

Domain Name System (DNS): One of the core parts of the infrastructure of the internet, the main task of which is to translate domain names into IP addresses. In this way, the requests users make by typing a web address into their browser can be correlated with a unique IP address in the network.

GATS agreement: The General Agreement on Trade in Services is an international treaty created by the World Trade Organization (WTO). It regulates cross-border trade in services and aims to liberalize it.

General Data Protection Regulation (GDPR): A legal act of the European Union which entered into force on 25 May 2018 in all Member States and harmonized the rules on the processing of personal data throughout Europe. It replaces Directive 95/46/EC, which dates back to 1995, and provides for heavy fines for possible infringements of European data protection law. According to the principle of lex loci solutionis, the regulation stipulates that non-European providers of goods and services such as internet platforms or cloud services operating within the EU are also automatically subject to the GDPR and must adapt their internal procedures and policies accordingly.

Geoblocking: A technology utilized on the internet to block certain content in certain geographic regions. For instance, some videos freely available on YouTube in Denmark or Poland cannot be viewed in Germany.

Hacktivism: A portmanteau of "hacking" and "activism" that designates political activism carried out via computers and networks.

Information intermediaries: Network platforms, search engines and other services that collect, structure and assign weight to information on the internet. In this respect, they provide a central function in rendering content on the internet searchable. For users they offer valuable orientation, but they also act as preselective filters. The algorithmic systems they employ are the subject of broad debate, particularly in connection with the spread of disinformation on social media.

International Telecommunications Union (ITU): An international organization dealing with the technical aspects of telecommunications. It has 191 members and is a specialized agency of the United Nations. It is based in Geneva.

Internet: A worldwide system connecting different computer networks with each other. It allows each computer connected to the internet to communicate with every other computer. The most important applications carried out over the internet are the World Wide Web as well as email and telephone services.

Internet Protocol (IP): The network protocol that forms the basis of the internet. It allows data packets from a computer connected to a network to be sent to another individual computer.

Internet service provider: A company providing access to the internet for its clients.

IP address: The unique address allocated to every computer connected to the internet, based on internet protocol.

National Security Agency (NSA): The largest U.S. intelligence agency, responsible for monitoring, decoding, and analyzing electronic communications worldwide. The vast extent of the surveillance it carries out was made public in 2013 via the revelations of a former employee, Edward Snowden.

Net neutrality: the technically equal treatment of data during its transmission on the internet, ensuring non-discriminatory access for all users. The so-called "best effort principle" is intended to ensure that access providers such as Deutsche Telekom, for example, are not allowed to restrict or slow the transmission of Netflix films, for example, in favor of their own content (e.g. streaming of football matches). According to network activists, a "zero rating," i.e. the free provision of content by internet service providers, also violates the principle of equal treatment.

Non-governmental organisation: Usually abbreviated to NGO, the term refers to any civilly organized association or interest group that is concerned with political topics such as the protection of human rights or the environment. Many large NGOs are granted an advisory or observer status at the UN and other international organizations.

Organisation for Economic Cooperation and Development (OECD): An international organization with 35 member countries that promotes democracy and free markets. It was founded in 1948 as the Organization for European Economic Co-operation (OEEC) and is based in Paris.

Roadmap: A term from international politics that designates a plan fora long-term political project that contains an overview of the steps necessary to reach the goal proposed.

Router: Network devices that transfer data packets between networks or between computers and networks. They are usually used to connect end devices such as personal computers or notebooks to the internet.

Switch: A device in network technology that connects different parts of a network with each other.

Think Tank: A term designating institutes, usually organized independently of the state, which participate in the political process in an advisory manner by creating studies, analyses, or potential strategies that analyze and address specific social, economic, or political questions.

World Trade Organization (WTO): An international organization founded in 1994 that is the successor of GATT and deals with trade and economic policy on a global scale. It is based in Geneva.

World Intellectual Property Organization (WIPO): An international organization founded in 1967 and based in Geneva. Its function is to secure intellectual property rights worldwide. It is a specialized agency of the UN and has 188 member states.

Whistleblower: A person with access to secret information belonging to a company, organization, or state agency who publishes this information in order to expose practices considered illegal or unethical. An EU directive on the protection of whistleblowers from 2019 must be translated into national law by the Member States over the next few years.

Whois: protocol used to retrieve information on internet domains and IP addresses and their owners. For data protection reasons, since 2010 the holders of .de domains can no longer be queried via the whois protocol, but only via the homepage of DENIC (Deutsches Network Information Center), which administers the top-level domain .de.

World Wide Web (WWW): An internet service created in 1989 by the English scientist Tim Berners-Lee, which makes available documents and other resources by means of websites connected to each other via hyperlinks. It is accessed via web browsers on users' end devices. The WWW is part of the internet, but is not identical to it.

Literature and links

Balleste, Roy: Internet Governance—Origins, Current Issues, and Future Possibilities, 2015.

Betz, Joachim and Kübler, Hans-Dieter: Internet Governance—Wer regiert wie das Internet?, 2013.

Centre for International Governance Innovation und Chatham House (eds.): Global Commission on Internet Governance—One Internet, 2016, https://www.cigionline.org/publications/one-internet-evidentiary-basis-policy-making-internet-universality-and-fragmentation.

Deloitte (ed.): Cyber Security Report 2019. First Part: Fake News und Schlüsseltechnologien—wachsende Herausforderungen, https://www2.deloitte.com/de/de/pages/risk/articles/cyber-security-report.html.

DeNardis, Laura: One Internet—An Evidentiary Basis for Policy Making on Internet Universality and Fragmentation. GCIG Paper No. 38, 2016.

DeNardis, Laura: The Global War for Internet Governance, 2014.

DeNardis, Laura: The Internet is Everything. Freedom and Security in a World with No Off Switch, 2020 (forthcoming).

Esch, Johanna: Internationale Internet-Governance. Das Internet als Herausforderung für etablierte Medienpolitik, in: Aus Politik und Zeitgeschichte 40-41 (2018), pp. 35-40, http://www.bpb.de/apuz/276561/internationale-internet-governance-das-internet-als-herausforderung-fuer-etablierte-medienpolitik?p=all.

Hölig, Sascha und Hasebrink, Uwe: Reuters Institute Digital News Report 2019 für Deutschland—Ergebnisse für Deutschland. In collaboration with Julia Behre, 6/2019 (Working Papers HBI no. 47), https://www.hans-bredow-institut.de/de/publikationen/reuters-institute-digital-news-report-2019-ergebnisse-fuer-deutschland.

Hofmann, Jeanette: Multi-Stakeholderism in Internet Governance: Putting Fiction into Practice, Journal of Cyber Policy, pp. 29-49 (2016), 10.1080/23738871.2016.1158303.

Hofmann, Jeanette: Constellations of trust and distrust in Internet governance, in: Europäische Kommission (ed.), Trust at Risk: Implications for EU Policies and Institutions, 2017, pp. 85-98, https://publications.europa.eu/en/publication-detail/-/publication/e512c11b-e922-11e6-ad7c-01aa75ed71a1/language-en/format-PDF/source-104354701.

Jaume-Palasi, Lorena and Pohle, Julia and Spielkamp, Matthias (eds.): Digitalpolitik. Eine Einführung. Published by Wikimedia Deutschland e.V. and iRights.international, supported by ICANN, 2017, https://irights.info/wp-content/uploads/2017/05/Digitalpolitik_-_Eine_Einfuehrung.pdf.

Kettemann, Matthias C.: Völkerrecht in Zeiten des Netzes. Perspektiven auf den effektiven Schutz von Grund- und Menschenrechten in der Informationsgesellschaft zwischen Völkerrecht, Europarecht und Staatsrecht. Published by FES Media Politics in the Department of Political Academy of the Friedrich-Ebert-Stiftung, 2015, http://library.fes.de/pdf-files/akademie/12068.pdf.

Kettemann, Matthias C.: Internationale Regeln für soziale Medien. Menschenrechte wahren und Desinformation bekämpfen, in: Global Governance Spotlight 2 (2019), https://www.sef-bonn.org/de/publikationen/global-governance-spotlight/22019.html.

Kleinwächter, Wolfgang: Internet Governance Outlook 2019: Innovative Multilateralism vs. Neo-Nationalistic Unilateralism, in: Circle ID (1-8-2019), http://www.circleid.com/posts/20190108_internet_governance_2019_innovative_multilateralism_vs_neo.

Kurbalija, Jovan: An Introduction to Internet Governance, 6th edition, 2014.

Masters, Jonathan: What Is Internet Governance?, 2014, https://www.cfr.org/backgrounder/what-internet-governance.

NETmundial (ed.): NETmundial Multistakeholder Statement, 2014, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

OECD (ed.): The Economic and Social Role of Internet Intermediaries, 2010, https://www.oecd.org/internet/ieconomy/44949023.pdf.

Schulz, Wolfgang and Dankert, Kevin: Die Macht der Informationsintermediäre. Erscheinungsformen, Strukturen und Regulierungsoptionen. Published by FES Media Politics in the Department of Political Academy of the Friedrich-Ebert-Stiftung 2016, https://library.fes.de/pdf-files/akademie/12408.pdf.

Weber, Rolf H.: Proliferation of ‚Internet Governance', 2014, http://ssrn.com/abstract=2809874.

Singer, Peter W. and Brooking, Emerson T.: LikeWar. The Weaponization of Social Media, 2018.

United Nations (ed.): The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation, 2019, https://eucyberdirect.eu/wp-content/uploads/2019/10/un-high-level-panel-digital-cooperation-2019.pdf.

Zuckerberg, Mark: A Blueprint for Content Governance and Enforcement (11-15-2018), https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634.

Further information on the internet

African Union (AU):
http://www.au.int

Council of Europe:
http://www.coe.int/de

Freedom on the Net:
https://freedomhouse.org/report-types/freedom-net

GATS Agreement:
http://www.bmz.de/de/themen/welthandel/welthandelssystem/WTO/GATS/index.html

International Telecommunication Union (ITU):
http://www.itu.int/en

Internet Corporation for Assigned Names and Numbers (ICANN):
https://www.icann.org

Internet Governance Forum (IGF):
http://www.intgovforum.org

Internet Governance Forum Deutschland (IGF-D):
http://www.intgovforum-deutschland.org

Internet-Governance-Radar
https://internet-governance-radar.de

Multistakeholder Advisory Group (MAG):
http://www.intgovforum.org/cms/mag

National Security Agency (NSA):
https://www.nsa.gov

NETmundial Initiative:
https://www.netmundial.org

Organization for Economic Cooperation and Development (OECD):
http://www.oecd.org

World Trade Organization (WTO):
https://www.wto.org

World Intellectual Property Organization (WIPO):
http://www.wipo.int

About the authors

Photo: Henning Lahmann

Henning Lahmann is Senior Policy Advisor at iRights.Lab. He worked for five years as a research assistant at the Walther Schücking Institute for International Law in Kiel and at the University of Potsdam. During this time he did his doctorate in international law on questions of transnational cyber security and the applicability of international regulations in cyberspace.

Photo: Die Hoffotografen / CC-BY-SA-4.0

Jan Engelmann Jan Engelmann works as a Policy Advisor at iRights.Lab and supports the management in strategic issues and organizational development. Previously, he worked as Managing Director for the Whistleblower Network, Social Reporting Initiative and Wikimedia Germany.

The Friedrich-Ebert-Stiftung

The Friedrich-Ebert-Stiftung (FES) is the oldest political foundation in Germany with a rich tradition in social democracy dating back to its foundation in 1925. The foundation owes its formation and its mission to the political legacy of its namesake Friedrich Ebert, the first democratically elected German President. The work of our political foundation focuses on the core ideas and values of social democracy—freedom, justice and solidarity. This connects us to social democracy and free trade unions. As a non-profit institution, we organize our work autonomously and independently. The FES promotes social democracy above all through its activities:

- Political educational work to strengthen civil society
- Policy advice
- International cooperation with foreign offices in more than 100 countries
- Support for talented young people
- The collective memory of social democracy with, among others, an archive and library

www.fes.de

Order print version/Contact

medienpolitik@fes.de
www.fes.de/medienpolitik

Online version of this publication:

Based on the guiding principle "digital policy means social policy," this publication follows the idea that internet governance affects everyone. An open, free and global internet is vital for all. Therefore, infrastructures of surveillance and censorship should not be established. For digital societies, the regulation of the "network of networks" has long since acquired a political dimension. Human and civil rights and questions of social, cultural and economic participation are on top of the agenda. This publication gives an overview of actors and areas of action and stresses that collective engagement is needed more than ever to further develop internet governance, to strengthen multistakeholderism as well as multilateralism and to hinder the fragmentation of the net.

Cover photo: Jan Zappner, re:publica / CC BY 2.0

FRIEDRICH EBERT STIFTUNG

ISBN 978-3-96250-505-9