KONRAD
ADENAUER
STIFTUNG

Internet Governance:
Past, Present and Future

By Wade Hoxtell and David Nonhoff

GPPi
GLOBAL PUBLIC POLICY
INSTITUTE

www.kas.de

Internet Governance: Past, Present and Future

By Wade Hoxtell and David Nonhoff

Acknowledgments

The authors would like to thank the following people for their input and feedback: Alexander Gaus, Niklas Kossow, Robert Morgus, Matt Noyes, Joel Sandhu, Christian Senninger and Sebastian Weise.

Contents

1. Introduction

The Internet, a global system of interconnected computer networks, is one of the most defining technologies of our time. Most aspects of our lives are touched in some form or another by the Internet, including our economic and financial systems, our social interactions, our education, work and civic participation, as well as the many services we use to complement our lives, from entertainment and banking services to booking travel. In many ways, the Internet has become an indispensable aspect of modern life – and peoples' dependence on the Internet and its ecosystem of services will only continue to grow.

Despite the constant and ubiquitous presence of the Internet, most people have little understanding about how this complex system actually works. Internet users, particularly in areas with highly reliable connections, take it for granted that everything simply works as expected. Yet, underpinning all technical infrastructure, applications, services and content is a complex system of institutions, actors, mechanisms, and rules that govern how the Internet works – termed "Internet governance." Internet governance is broadly defined as the processes that influence how the Internet is managed – locally, nationally, regionally and globally.[1] The United Nations Working Group on Internet Governance (WGIG) defined Internet governance in 2005 as "the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programmes, that shape the evolution and utilization of the internet."[2] While it took until 2005 to reach agreement on this definition, the principles, rules, norms and processes that underpin the Internet have been evolving for decades and will continue to evolve.

Yet, there are two key challenges that are posing a threat to the free and open model of the Internet. First, states such as Russia and China are challenging the multistakeholder model of Internet governance. Whereas the multistakeholder model places responsibility for critical decisions on the future of the Internet into the hands of a wide range of stakeholders from the public, private, civil society and technical sectors, Russia and China seek more (inter)governmental control of the Internet and are actively promoting a more authoritarian and illiberal form of the Internet that restricts access to information and represses citizens.

Second, the free and open Internet that is built upon the idea of largely uninhibited information flows is being threatened by efforts to control and limit the types of information accessible to users. This "fragmentation" has thus far mainly occurred *on* the Internet in the form of the regulation of content through, for example, censorship or, in the case of overturning net neutrality, the erosion of the principle of equal access. Yet, there is also a risk of fragmentation *of* the Internet, namely the introduction of new physical infrastructure that could threaten the existence of a global network and instead introduce a number of separate networks with little to no information exchange.

The aim of this study is to present these challenges and their potential impact on the future of Internet governance. Chapter 2 provides a brief history and definition of Internet governance as well as summarizes how this system currently functions and the key actors involved. Chapter 3 presents key challenges to Internet governance and their potential implications for the free and open Internet. Chapter 4 provides two different outlooks for how the Internet and its governance could look in the future, specifically, what a best and worst case could look like. Chapter 5 concludes with policy recommendations for Europe and Germany.

[1] Internet Society (2019). *Internet Governance.* Retrieved 14 February 2019, from https://www.internetsociety.org/issues/internet-governance/.

[2] Working group on Internet Governance (WGIG) (2005). *Report of the Working Group on Internet Governance,* Château de Bossey, June 2005. Retrieved 01 February 2019 at https://www.wgig.org/docs/WGIGREPORT.pdf.

2. A Brief History of Internet Governance

The core concept of the Internet as a decentralized network of networks was born in the United States in the 1950s and 1960s due to the perceived threat of a Soviet nuclear attack on the country's centralized communication systems.[3] The idea was to build a decentralized system of communication that would utilize a "web" rather than a central hub. In such a system, messages could be sent through a large network of carrier lines without having to pass through a central and easily destroyable hub, allowing for different pathways to the destination.[4]

The first such decentralized system was the Arpanet, a project of the Advanced Research Projects Agency (ARPA) under the US Department of Defense, which connected the computers of four universities in the United States (US).[5] In the following decades, as the Cold War threat diminished, the Department of Defense lost interest in the idea of a decentralized communications network and left the remnants of what they had created to "excited students who wanted to connect computers and test and develop something new."[6]

The US government's abdication of primary responsibility for designing and managing the early Internet was a crucial development. The decision laid the foundation for two key traits that have long been embedded into the DNA of the Internet, namely, a multi-stakeholder governance model and the idea that the Internet should be "free and open". With respect to the former, the multi-stakeholder governance model enables a variety of actors or stakeholders – governments, the private sector, the technical community and civil society – to come together to make decisions for how the Internet should work. In this context, early governance efforts were primarily limited to technical issues such as assignment of globally unique identifiers on the Internet, for example, the domain names of our favorite websites, or technical standards necessary for the interoperability of different networks. Early Internet pioneers at university campuses as well as non-governmental organizations (NGOs) governing technical aspects of the Internet, such as the Internet Engineering Task Force (IETF), the Internet Architecture Board (IAB), or the Internet Corporation for Assigned Names and Numbers (ICANN), believed in open, non-proprietary standards to allow devices, services, and applications to work together across a wide and dispersed network of networks.[7] Their modus operandi is best described as a transparent, open, and bottom-up consensus-building process. They were skeptical towards government influence and as David Clark, one of its pioneers, famously declared: "We reject: kings, presidents and voting. We believe in: rough consensus and running code."[8]

Such attitudes underscored the idea that the Internet should be both free and open to the largest degree possible. Born out of libertarian ideals in the United States, the "free and open" credo of the early Internet meant that information should flow freely across all networks, that all should have equal access to use the Internet in almost any way imaginable, and with limited government interference.[9] This had a number of critical implications. First, from a technical standpoint, it meant that different networks with different transmission technologies could connect into one large global network, allowing for internetwork communication of independent and physically differing networks through a common protocol – the Transmission Control Protocol/Internet Protocol (TCP/IP).[10] Second, from an economic, social and political standpoint, this approach was critical for allowing anyone with a computer and an internet connection to play a role in building the identity of the Internet. As such, it served as a key driver of the Internet's astonishing growth and its role as, for example, an engine for economic growth and international trade, a vehicle for new technological development, and as a platform for exercising human rights such as the freedoms of speech and assembly.[11]

Today, Internet governance encompasses the entire mix of issues that determine the Internet experience at the local, national, regional and global levels – ranging from the technical side, such as interoperability standards, to politicized issues such as censorship, misinformation campaigns and net neutrality, among many others.

How does Internet governance work?

Internet governance is composed of three broad areas: 1) The tools that govern the functioning of the Internet and behavior on it; 2) the layers upon which these tools are used at the local, national, regional and global levels; and 3) the actors that are involved in shaping and applying these rules.

First, the tools of Internet governance take the form of laws, policies, technical standards or codes of conduct that are formed, monitored and enforced by numerous actors. For example, policies regarding public investment into the maintenance, expansion, and upgrading of infrastructure are mostly set by governments, as is the case currently with rollout of the 5G mobile data standard. Non-governmental organizations are often primarily responsible for ensuring technical coordination and compatibility. For example, the non-profit Internet Corporation for Assigned Names and Numbers (ICANN) manages the assignment of domain names and IP addresses while the Internet Engineering Task Force (IETF), an international non-profit organization with open membership, promotes voluntary Internet standards that ensure technical coordination and compatibility.[12] Private sector companies that create the software that defines the Internet experience are often responsible for developing the codes of conduct for the usage of these applications, whereas governments play a role in regulating content online as illustrated, for example, by Chinese censorship laws.

Second, these tools are applied across different ‘layers’ that make the entire functioning and usage of the Internet possible:[13]

The infrastructure layer represents the physical structure needed to send data from one point to the other in the giant network of the internet. It consists of all of the hardware needed for creating and passing information from one point to another, for example, computers, terrestrial and undersea cables, satellites, exchange points, wireless systems and wires. In effect, the infrastructure layer of the Internet is comparable to the airplanes, freighters, delivery trucks and post boxes required for the postal system to function.

The logical layer provides the instructions for how this information travels through the infrastructure layer and ensures compatibility between different networks. Most importantly, it is responsible for governing the domain name system (DNS) – a system that translates domain names to IP addresses. The role of the logical layer is roughly equivalent to the system for regulating the sizes of mail packages, the usage and acceptance of stamps internationally as well as ensuring that the respective pieces of mail are travelling in the correct direction.

The applications layer of the Internet is where we find the many pieces of software and applications that allow us to both access the Internet via our electronic devices as well as leverage different online services. This includes, for example, e-mail software, internet browsers, Skype or games on mobile phones. Fundamentally, these applications enable direct communication between different networked devices and users. As such, the role of the application layer of the Internet is comparable to those of the postcard and the tool we use to write on them, such as a pencil or pen.

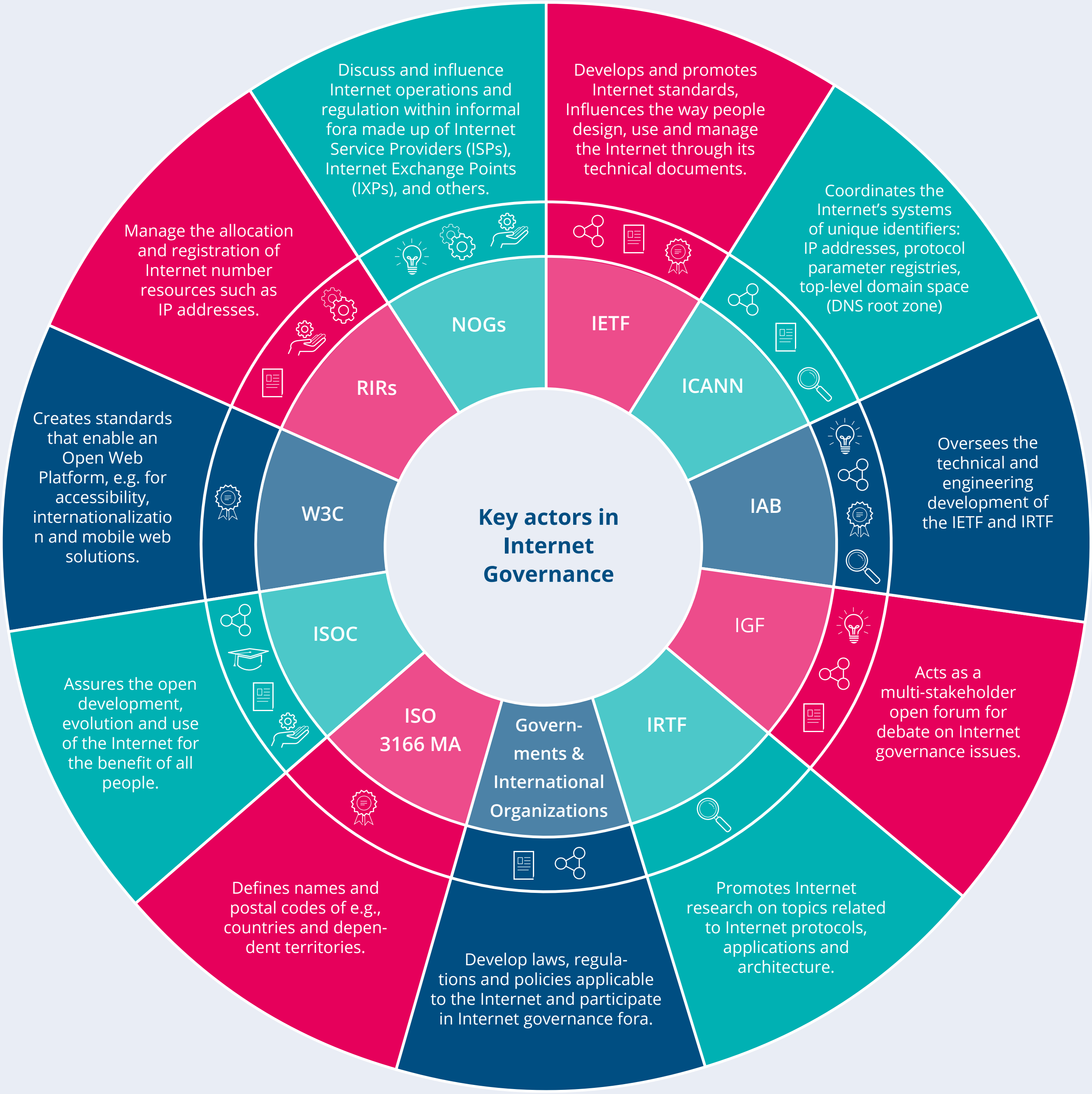
The content layer of the Internet is all of the information that can be found within the application layer. This includes, for example, the text on websites, videos in news media applications, images on Instagram, and the audio content of your favorite podcast. In the postal service example, the content layer is equivalent to the message that is written on a postcard.

In its early stages, the Internet was predominantly viewed as a purely technical infrastructure and, as such, Internet governance primarily took place along the infrastructure and logical layers.[14] As such, it concerned governance of the Internet.[15] This began to change rapidly when commercial use of the Internet began in earnest in the 1990s. With the numbers of Internet users and uses rising sharply, new challenges arose. Mere maintenance and regulation of the infrastructure and logical layer were increasingly regarded as insufficient and the main concerns of Internet governance shifted to the layers of applications and content – namely governance of what is on the internet. As the different types of content proliferated, it became increasingly important to consider how this content either abided or conflicted with existing laws outside of the virtual world, for example, freedom of expression, consumer protection, and privacy, among many other issues.[16]

Further, Internet governance happens at the global, regional, national and local levels. As a basic rule, the first two layers of Internet governance, the infrastructure and the technical layer, have a global approach. Protocols, cables, and routers are maintained collaboratively by the countries involved due to the value and need to keep the Internet functional as a cross-border and global technical structure.[17] The application and content layers, on the other hand, are more susceptible to national or local governance mechanisms for regulating, for example, the content that is allowed to be published or viewed online. Internet users are therefore always subject to their home countries' laws and regulations when going online.

Finally, a number of actors are involved in applying these rules. As discussed above, the multistakeholder model means that no single stakeholder has a leading role in governing the Internet. In 2005, the World Summit on Information Society produced the Tunis Agenda for Information Society, a consensus document which stated that "the international management of the Internet should be multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organizations. It should ensure an equitable distribution of resources, facilitate access for all and ensure a stable and secure functioning of the Internet, taking into account multilingualism." This principle is perhaps best illustrated by the formation, also in Tunis in 2005, of the Internet Governance Forum (IGF) – the most important forum for information and best-practice sharing among Internet stakeholders from governments, international institutions, non-governmental organizations, companies and other civil society actors. A more comprehensive list of actors and how they contribute to Internet governance can be found in Infographic 1 below.

Infographic 1: Who runs the Internet?



Key actors in Internet Governance

IETF

Develops and promotes Internet standards, Influences the way people design, use and manage the Internet through its technical documents.

ICANN

Coordinates the Internet's systems of unique identifiers: IP addresses, protocol parameter registries, top-level domain space (DNS root zone)

IAB

Oversees the technical and engineering development of the IETF and IRTF

IGF

Acts as a multi-stakeholder open forum for debate on Internet governance issues.

IRTF

Promotes Internet research on topics related to Internet protocols, applications and architecture.

Govern-ments & International Organizations

Develop laws, regula-tions and policies applicable to the Internet and participate in Internet governance fora.

ISO 3166 MA

Defines names and postal codes of e.g., countries and depen-dent territories.

ISOC

Assures the open development, evolution and use of the Internet for the benefit of all people.

W3C

Creates standards that enable an Open Web Platform, e.g. for accessibility, internationalizatio n and mobile web solutions.

RIRs

Manage the allocation and registration of Internet number resources such as IP addresses.

NOGs

Discuss and influence Internet operations and regulation within informal fora made up of Internet Service Providers (ISPs), Internet Exchange Points (IXPs), and others.

IETF	Internet Engineering Task Force
ICANN	Internet Corporation for Assigned Names and Numbers
IAB	Internet Architecture Board
IGF	Internet Governance Forum
IRTF	Internet Research Task Force
ISO 3166 MA	International Org. for Standardization, Maintenance Agency
ISOC	Internet Society
W3C	World Wide Web Consortium
RIRs	Five Regional Internet Registries
NOGs	Internet Network Operator Groups

Advice

Community Engagement

Policy

Standards

Operations

Education

Research

Services

Graphic source: ICANN (2013). Who Runs the Internet? *Retrieved 13 June 2019, from https://www.icann.org/en/system/files/files/governance-06feb13-en.pdf.*

[3] Bygrave, L. A., Bing, J. (2009). *Internet Governance: Infrastructure and Institutions.* Oxford University Press.

[4] Unknown author (2016). *Understanding Media and Culture: An Introduction to Mass Communication.* Chapter 11.2: The Evolution of the Internet. University of Minnesota Libraries Publishing edition, available at https://open.lib.umn.edu/mediaandculture/.

[5] Ibid.

[6] Kleinwächter, W. (2015). *The history of Internet Governance,* lecture at Summer Schools on Internet Governance. Retrieved 06 February 2019, from https://www.youtube.com/watch?v=5QUrkRtC2Js.

[7] Internet Society Website (2019). Open Internet Standards Chapter Toolkit. Retrieved 18 March 2019, from https://www.internetsociety.org/chapters/resources/open-internet-standards-chapter-toolkit.

[8] Van Beijnum, I. (2011). *25 years of IETF: setting standards without kings or votes.* ArsTechnica. Retrieved 18 March 2019, from https://arstechnica.com/tech-policy/2011/01/25-years-of-ietf-setting-standards-without-kings-or-votes/.

[9] Hoxtell, W. (2019). *The Web at 30: What's the State of Internet Governance?* Retrieved 14 March 2019, from https://www.gppi.net/2019/03/12/the-web-at-30.

[10] Cerf, V. G. et al. (1997). *Brief History of the Internet. Internet Society.* Retrieved 05 February 2019, from https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf.

[11] Benner, T., Hohmann, M. (2018). *Getting „Free and Open" Right. How European Internet Foreign Policy Can Compete in a Fragmented World.* GPPi Policy Paper. Retrieved 15 February 2019, from https://www.gppi.net/media/Hohmann_Benner_2018_European_Internet_Foreign_Policy.pdf.

[12] See: https://www.icann.org/ and https://www.ietf.org/. Accessed March 4, 2019.

[13] This typology has been used by many scholar of Internet governance. See, for example, Benkler, Y. (2000). *From Consumers to Users: Shifting the Deeper Structures of Regulation Towards Sustainable Commons and User Access.* Federal Communications Law Journal: Vol. 52 : Iss. 3, Article 9.

[14] Niesyto, J., Otto, P. (2017). *Who governs the internet? Players and fields of action.* Friedrich-Ebert-Stiftung, retrieved 20 March 2019, from http://library.fes.de/pdf-files/akademie/13910.pdf.

[15] Kleinwächter, W. (2015). *The history of Internet Governance, lecture at Summer Schools on Internet Governance. R*etrieved 06 February 2019, from https://www.youtube.com/watch?v=5QUrkRtC2Js.

[16] Ibid.

[17] Niesyto, J., Otto, P. (2017). *Who governs the internet? Players and fields of action.* Friedrich-Ebert-Stiftung, Retrieved 20 March 2019, from http://library.fes.de/pdf-files/akademie/13910.pdf.

3. Two Key Challenges for Internet Governance

As the economic, political and social importance of the Internet, as well as the number of users and uses, has grown, the original libertarian credo that stressed a "hands-off" approach vis-à-vis governments has become increasingly unrealistic. Numerous examples exist that illustrate the need to find a balance between internet freedom and regulation. For example, while privacy, anonymity, and the protection of private communication can be important with respect to the formation of public opinion and the possibility for social or political dissent, it has also become clear that, in some instances, there are good reasons for exposing those who post criminal content, threaten other users or circulate hate speech.[18] Further, misinformation and intransparent advertising, to take two examples, have proven to be powerful and inexpensive tools in the competition between liberalism and authoritarianism. As such, the need for regulating such content has only become more pronounced.[19]

As such examples show, the Internet and Internet governance have increasingly become political issues and, subsequently, have led to a growing role for governments in regulating the online experience. Yet, approaches for regulation vary wildly. Whereas European countries have come forward with legislation that tries to protect privacy and copyright laws and contain hate speech, other states such as China actively censor the Internet on both the application and the content layer and create sophisticated and all-encompassing means of surveillance and control which threaten freedom, democracy and pluralism. Whereas authoritarian states are able to impose such measures without much resistance, regulating the Internet is a delicate matter for liberal democracies. It is particularly difficult for liberal democracies to regulate speech online, enforce copyright laws, and infringe on people's privacy in the name of security as illustrated by, for example, new European Union (EU) legislation for enforcing copyright laws online that sparked huge outrage, especially among young voters who argue that such regulation would curtail free speech.[20]

Given that the importance of the Internet will continue to grow in the coming years, such issues – and new ones not yet anticipated – will become even more pronounced. In this respect, two key challenges for Europe moving forward will be to, first, preserve and advance the multi-stakeholder governance model and, second, find the appropriate balance between the "free and open" ideal and the need for regulation.

Multistakeholder vs. (Inter)governmental Control

One of the most crucial aspects of Internet governance is the question of power: Who should have how much influence and control over the Internet's layers and decision-making processes? This debate has two camps. On one hand, the United States, many Western countries, as well as private companies favor the multistakeholder approach where all stakeholders affected by the Internet should also be allowed to participate in its governance. The advocates of this view believe that the very nature of the Internet as a decentralized, global, and open system makes it too complex to be governed by governments alone and, as such, giving states too much control would pose the danger of restricted civil rights and liberties.[21] On the other hand, governments such as China and Russia demand an increasing role for governments in Internet governance, particularly with regards to fighting (cyber) terrorism and controlling data. They contend that governments have more legitimacy than non-governmental organizations or the private sector in governing something as important as the Internet. Further, they not only promote the idea of 'cyberspace sovereignty' where states exercise control over the Internet within their borders, but they are also trying to export this model to other countries.[22]

The ideological war between these camps has been going on for decades, as illustrated for example by repeated attempts to shift responsibility of the domain name system (DNS) from ICANN, a non-profit organization, to the International Telecommunications Union (ITU), a United Nations organization. The DNS is one of the most critical internet resources as it provides a unique identifier to each website and enables the usage of e-mail addresses. Keeping it operational and secure is therefore of crucial interest to governments. Yet, at the same time, yielding more power to governments through the ITU creates the risk of increased influence of countries that seek to restrict civil rights and liberties on the Internet.

Yet, the multistakeholder model is not immune to criticism. The selection procedures for ICANN's board members, for example, remain unknown to the public. Other commentators lament that as a non-governmental, private organization, ICANN is in an ill-suited position to fulfil a public interest function as it lacks perceived legitimacy from states and Internet users.[23] Advocates for larger government involvement argue that the ITU, with its 193 member-states with voting rights and more than 700 sector members and associates, can more democratically manage the DNS than ICANN or other unelected entities.[24] Further, the Internet Governance Forum (IGF), the main mechanism for information sharing and debate on Internet governance, does not have binding decision-making authority and its influence on national-level policymaking is limited. The IGF also suffers from both criticisms of its effectiveness as well as a weak participation by actors from developing countries or from those who otherwise lack the resources to bring their voices and concerns to the fore.[25]

Free and Open vs. Fragmentation

Advocates of the multistakeholder Internet governance model usually also argue for a globally free and open Internet. In the context of Internet governance, "free and open" suggests that information should flow freely across networks with no limitations, that everyone should have equal access to the Internet and that they should be able to use it in any way they see fit, without special permission by anyone. Implicitly, this entails a 'hands-off' approach that precludes too much government intervention into the management, development and regulation of the Internet. This approach was critical in the Internet's early development for allowing everyone and anyone to explore the entire realm of possibilities that it could offer. It played a key role in the Internet's astonishing growth, its role as an engine for new business models, in international trade, and as a platform for exercising human rights such as the freedoms of speech and assembly.[26]

Over the past years, however, due to increased regulation of the Internet around the world, a growing number of commentators have expressed concerns that the Internet might be fragmented into several loosely coupled networks or islands of connectivity.[27] Such Internet fragmentation, understood as a departure from the fundamentally free and open approach to Internet governance, can be differentiated into at least two forms: Technical fragmentation and government fragmentation.[28] Technical fragmentation refers to fragmentation of the Internet, namely at the basic infrastructure and logistic layers of the Internet of wires, protocols and root servers. Widespread technical fragmentation would eliminate the global "network of networks" and replace it with a kind of multiverse of local, national or regional networks with no information flows between them.[29]

Government fragmentation, on the other hand, affects the content and application layers and as such refers to fragmentation *on* the Internet. It refers to government policies or laws that influence the degree to which it is possible to create, distribute or access information online.[30] This include the regulation of content, blocking access to certain services or websites based on their location, or by using the Internet as means for mass surveillance. Increased government fragmentation could lead to a multitude of national Internets with so-called digital borders. To some degree, this is already a reality. Everybody who has ever tried to watch German public television online from abroad will have experienced the effects of geo-blocking. Also, from within Europe, it can sometimes prove difficult or impossible to reach non-European websites that struggle with the implementation of EU data or privacy legislation.

Such restrictions cut against the original vision of a free and open Internet. Yet, a romanticized vision of the Internet as a libertarian Wild West with no control or regulation at all is naïve and the idea of a free and open Internet to some extent flawed. The Internet has long been regulated to some degree and this is neither surprising nor regrettable regarding its growth and its importance. Some regulation is essential to ensure that the rights we enjoy in the physical world are also protected in the virtual one.[31] In addition to some of the measures detailed above, democratic states, for their part, have implemented a number of laws that further regulate the Internet. Germany has prominently tried to tackle hate speech online with its network enforcement law which can be praised as an active measure against online crime, but also criticized for privatizing law enforcement and unintentionally contributing to the fragmentation of content whereby online platforms utilize preemptive or reactive censorship to avoid fines.[32]

Authoritarian governments, like China, Russia, and Iran have for a long time been at the forefront of regulating the Internet and cutting against the idea of a free and open global network of networks. Free flow of data and information poses a direct challenge to their political systems and hence, they never ascribed to the narrative of a free and open Internet.[33] These states have developed vast capabilities for information control and have begun promoting their alternative narrative of a state-dominated Internet governance in opposition to the free and open multistakeholder model. This poses a problem for liberal democracies, since authoritarian states are not only restricting information flows within their own countries and using the Internet as a tool for repressing their citizens, they are exporting this model on Internet governance to other countries and also offer the technologies to do so.[34] In doing so, they are actively promoting greater Internet fragmentation and thus a future that consists not of one global Internet, but rather a multitude of national or sub-national Internets.

[18] Gruber, B., Jaume-Palasí, L., Leidel, S., & Spielkamp, M. (eds.) (2016). *Guidebook Internet Governance: Media freedom in a connected world.* DW Akademia. Retrieved 18 March 2019, from https://www.dw.com/downloads/30373593/dwaguidebook-internet-governancefinal.pdf

[19] Kagan, R. (2019). *The strongmen strike back.* The Washington Post, The Opinions Essay. Retrieved 18 March 2019, from https://www.washingtonpost.com/news/opinions/wp/2019/03/14/feature/the-strongmen-strike-back/?utm_term=.53991c1517a5

[20] Vaughan-Nichols, S. J. (2019). The EU's new copyright laws threaten to destroy the internet. ZDNet Blog Networking. Retrieved 20 March 2019, from https://www.zdnet.com/article/the-eus-new-copyright-laws-threaten-to-destroy-the-internet/

[21] See, e. g.: Kleinwächter, W. (2016). *Wer regiert das Internet? Internet Governance auf dem Prüfstand.* Vereinte Nationen 2/2016, p. 69. Retrieved 15 February 2019, from https://zeitschrift-vereinte-nationen.de/fileadmin/publications/PDFs/Zeitschrift_VN/VN_2016/Heft_2_2016/05_Beitrag_Kleinwaechter_VN_2-16_11-4-2016.pdf and Niesyto, J., Otto, P. (2017). *Who governs the internet? Players and fields of action*. Friedrich-Ebert-Stiftung. Retrieved on 15 February 2019, from http://library.fes.de/pdf-files/akademie/13910.pdf

[22] Sacks, S. (2018). Beijing Wants to Rewrite the Rules of the Internet. The Atlantic, 18 June 2018. Retrieved 01 March 2019, from https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/

[23] Gross, R. (2014). *Comments on Enhancing ICANN Accountability,* ICANN. Retrieved 11 March 2019, from http://forum.icann.org/lists/comments-enhancingaccountability-06may14/msg00036.html

[24] Savage, J. E., and McConnell, B.W. (2015). *Exploring Multi-Stakeholder Internet Governance.* EastWest Institute, January 2015. Retrieved 11 March 2019, from https://www.files.ethz.ch/isn/188305/governance.pdf

[25] Spielkamp, M. (2016). Internet governance – why we should care. Interview for Deutsche Welle Akademie. Retrieved 20 March 2019, from https://www.dw.com/en/internet-governance-why-you-should-care/a-19320659. For more information on the shortcomings of the IGF and potential solutions, see also United Nations (2019). *The age of digital interdependence.* Report of the UN Secretary-General's High-level Panel on Digital Cooperation. Retrieved 13 June 2019, from https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf.

[26] Hoxtell, W. (2019). *The Web at 30: What's the State of Internet Governance?* Retrieved 14 March 2019, from https://www.gppi.net/2019/03/12/the-web-at-30.

[27] Drake, W. Cerf, V., & Kleinwächter, W. (2016). *Internet Fragmentation: An Overview*, Future of the Internet Initiative White Paper, World Economic Forum, January 2016. Retrieved 11 March 2019, from http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

[28] Ibid.

[29] Hoxtell, W. (2019). *The Web at 30: What's the State of Internet Governance?* Retrieved 14 March 2019, from https://www.gppi.net/2019/03/12/the-web-at-30.

[30] Drake, W. Cerf, V., & Kleinwächter, W. (2016). Internet Fragmentation: An Overview, Future of the Internet Initiative White Paper, World Economic Forum, January 2016. Retrieved 11 March 2019, from http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

[31] Hoxtell, W. (2019). *The Web at 30: What's the State of Internet Governance?* Retrieved 14 March 2019, from https://www.gppi.net/2019/03/12/the-web-at-30.

[32] Kossow, N., & Webster, G. (2017). *The Pitfalls of Germany's New Hate Speech Law. Transatlantic Digital Debates 2018 podcast*. Retrieved 13 March 2019, from https://www.gppi.net/2017/07/19/the-pitfalls-of-germanys-new-hate-speech-law

[33] Benner, T., Hohmann, M. (2018). *Getting „Free and Open" Right. How European Internet Foreign Policy Can Compete in a Fragmented World.* GPPi Policy Paper. Retrieved 15 February 2019, from https://www.gppi.net/media/Hohmann_Benner_2018_European_Internet_Foreign_Policy.pdf

[34] Morgus, R., Woolbright, J. & Sherman, J. (2018). *The Digital Deciders – How a group of often overlooked countries could hold the keys to the future of the global internet.* New America report. Retrieved 20 March 2019, from https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/

4. Internet Governance in 2035: Best and Worst Cases for Europe

Given the speed of technological change and the vast opportunities being opened up by new technologies, forecasting what the Internet will look like in 15 years is an impossible task. Nevertheless, in order to preserve and advance the best aspects of the Internet while protecting against the worst, it can be enlightening to imagine different futures. Presented below are two different cases. The first case, called "A healthy and prosperous Internet for all", imagines a future Internet that is most closely aligned to the European best interest. The second case, "The demise of the free and open Internet", on the other hand, presents a situation that, from a European perspective, would be catastrophic.[35]

Best case: A healthy and prosperous Internet for all

By 2035, the European vision of a reasonably regulated, free and open Internet underpinned by a robust multi-stakeholder Internet governance model is on the march. Despite some national variations across the world, regulatory frameworks for Internet governance are increasingly rooted in a set of commonly accepted principles that protect the inviolability of the Internet as a global network of networks, where information flows freely, where the democratic rule of law, individual rights and freedoms are protected online. Fragmentation across the different layers of the Internet was largely avoided, likely as a result of two key developments: 1) the economic and social consequences of information became tangible following attempts by several Latin American countries to implement wide-scale restrictions and 2) China and Russia stopped actively exporting their vision of a government-controlled Internet and turned inward to deal with rising domestic challenges to this model. Citizens across the world, with a few national exceptions, enjoy a universal right of access to information. The rapid deployment and blanket reach of satellite-based Internet services has provided every citizen of the world with the opportunity to take advantage of cheap and reliable Internet access.

The European Internet economy has emerged as a hotbed of innovation for startups and large technology companies alike due to its efforts to promote fair competition and uphold privacy and the responsible handling of data. By successfully realizing the EU digital single market through the unfettered movement of persons, services and capital across national borders, the ecosystem of public, private and civil society actors within Europe began to thrive. As a result, the EU was able to leverage its normative power and its clout as the world's biggest economic bloc to more effectively market its vision of a free and open Internet, underpinned by fair regulation, worldwide.

While contenders of this vision, particularly Russia and China, continue to exert almost complete governmental control over information flows within their borders, this is beginning to change as their national technology champions, together with public sentiment, have convinced the respective governments to ease some information restrictions. In addition, as highlighted above, their efforts to strengthen intergovernmental control over the Internet as well as export this vision to other states have failed. While Europe's success in developing a robust Internet economy as well as its strong advocacy efforts within the Internet Governance Forum (IGF) played a key role in countering these attempts, ultimately market forces proved much more convincing. As developing and emerging countries increasingly closed the digital divide and experienced rapid economic growth due the launch of entirely new domestic and internationally-oriented service sectors, it became increasingly clear that the economic, political and social costs of information isolation and manipulation would only stifle their progress.

Moreover, the IGF evolved from its role as an information-sharing and discussion forum into a more robust platform for negotiating the major decisions with respect to Internet governance. While the IGF remains a deliberative and not a decision-making forum, the successful efforts of the IGF to become more effective, transparent and accountable platform with wide participation from all regions and stakeholder groups makes it the de facto arena for inspiring and catalyzing policy at the national level. The annual Forum regularly attracts minister-level participation and now serves as a key forum for high-level discussions and decision-making on digital policy. Its biggest achievement, however, has been its increasingly successful efforts to vertically integrate the global forum with its national spin-offs across the world. Such efforts of linking together the multitude of stakeholders responsible for different tasks at international and national levels, from all relevant sectors including the general public, have created a highly stable system of checks and balances within global and national Internet governance systems.

Further, the IGF has become increasingly adept at utilizing these national networks in order to coordinate international, multistakeholder consultation processes for gathering input from Internet stakeholders and feeding this input into its activities. In addition to extending the feeling of Internet ownership to citizens across the world, these processes also help ensure that all crucial decisions are taken with the common good in mind. Another key triumph in this respect was the IGF's development of a policy advisory committee that provides guidance and tools to aid national governments in their efforts to create responsible domestic Internet regulation that does not damage the Internet as a global resource or otherwise cut against human and digital rights. Interestingly, the technical interoperability that allowed for different networks to share information with one another inspired the adoption of a parallel and mutually reinforcing system of political and legal interoperability for protecting the Internet as a public good.

Finally, given the astonishing speed of the development and deployment of new technologies, services and business models together with high levels of economic growth, even large and powerful technology companies have come to embrace stronger regulatory frameworks in order to ensure continued stability in the global Internet ecosystem. In particular, the battle over net neutrality was finally put to rest as governments across the world, lobbied heavily by civil society organizations and the general public, agreed to codify net neutrality, among other principles, into a binding international treaty on digital rights. Moreover, in order to address rising concerns about power and corporate influence in the democratic process, a number of Internet giants took it upon themselves to institute measures of self-regulation as a means to preempt sweeping antitrust legislation. These actions opened up a more level playing field and reduced barriers to market entry for small companies that ultimately led to a boom in the development of innovative new products and services.

Worst case: The demise of the free and open Internet

In 2035, the European vision of a free and open Internet is collapsing. Technological advances in microprocessor technology, power efficiency and next generation mobile networks, as well as large cost reductions, have facilitated the Internet of Things revolution and led to a rapid transformation of virtually all sectors of society and people's lives. Yet, the benefits are increasingly being outweighed by the risks. In particular, the exponential increase in personal data, usage statistics and geolocation information collected by not only large technology companies, but also smaller companies producing apparel, appliances, food and beverages, among many other industries whose products are essential to our well-being, have led to alarming abuses of privacy and rapidly increasing instances of cybercrime and fraud across the world. As a result, citizens around the world, particularly in Europe, have lost trust in their governments' ability to solve the problem and are increasingly gravitating towards political extremism.

In response to this, governments around the world, including in Europe, have taken a heavy-handed approach to regulation that has not only contributed to neutering the innovative potential of the once free and open Internet, but also increasingly infringed upon human and digital rights of their respective citizens. In particular, efforts to thwart cyberattacks from state and non-state actors alike have led to a downward spiral where governments have introduced ever-more intrusive forms of surveillance as well as sweeping data-sharing agreements with private companies. In addition, most national governments have deployed sophisticated and unaccountable artificial intelligence systems to act as a filter for information flows into and out of networks.

These efforts, among others, proved to be a major driving force for fragmentation of the Internet, both with respect to increased restrictions on information flows as well as the creation of separate physical network infrastructures. The once global network of networks has become a collection of isolated networks with either limited and highly-controlled or no information flows between them as governmental efforts to align communication infrastructure with their national borders expanded. In addition to national efforts at controlling information flows, an increasing number of organizations, and even some municipalities, have started to operate self-governed proprietary networks using, in some cases, satellite-provided Internet service. Information discrimination has become rampant since the collapse of net neutrality rules worldwide in the mid-2020s and Internet service providers sell priority bandwidth to the highest bidder. Access prices have shot up and affordable connections are notoriously unreliable and slow, amplifying social justice concerns as well as stifling new market entrants, competition and innovation.

Further, the technical and legal interoperability of different networks has suffered as a result of the proliferation of incompatible and proprietary networks, making it ever harder or impossible to access websites, applications and content across national or, increasingly, subnational and corporate borders. As national digital sovereignty efforts expanded and governmental control over information flows increased, the economic implications have been profoundly negative, with some fearing an unprecedented global recession as a result of stifled trade and flows of capital, data and services. While the European Internet ecosystem remains relatively free and open, it is becoming ever harder for companies of all kinds to expand beyond their national jurisdictions, further restricting competition and innovation. In addition, European efforts to expand upon its General Data Protection Regulations (GDPR) through a complex patchwork of laws ultimately proved extremely unpopular among European citizens and companies due to, among other issues, the tedious user experience of Internet and service usage. A side-effect of this process was the rolling back of existing GDPR regulations, most notably those requiring fair, transparent and purpose-limited processing of personal data.

In addition to a tiered pricing system for Internet access, user bases are also segmented between those that have the resources to protect themselves against violations of rights and privacy and those who do not. While some service providers, software and hardware exist to protect users from, for example, surveillance and data collection activities, the high cost makes it available to the financially well-off. This privacy inequality is leading to a rapid disconnection of many users from all networks in what is popularly known as ‘device divestment’. This and other forms of social unrest in response to government infringement upon individual freedom and human rights have led many governments to double-down on their efforts by implementing measures from illiberal and authoritarian playbooks in order to suppress citizen criticism and opposition to their policies in order to stay in power. Moreover, while (inter) governmental control over Internet policy has grown, there has been no major anti-monopoly regulation in any country to curb the power of large technology companies due to their vast and unfettered lobbying expenditures, contributions to political campaigns and the financing of favorable research. These monopolistic platforms are actively hampering competition and, for those competitors that do manage to break into the market, most are quickly acquired and integrated into existing Internet giant ecosystems.

The severity of these developments played a major role in, and at the same time were accelerated by, the demise of the multistakeholder Internet governance model and the diminished significance of the Internet Governance Forum. This occurred because the long-standing efforts by states such as Russia and China to shift control of Internet policymaking to the International Telecommunications Union (ITU) finally proved successful as governments across the world sought a higher level of control in an effort to address security issues and restore user trust in the Internet. As a body subjected to intergovernmental political oversight, high bureaucratic demands and inefficient operating practices, among other issues, the ITU has proven extremely ineffective at keeping up with the rapid pace of technological change and has proven largely irrelevant in Internet policymaking. As a result, global Internet governance efforts that had once protected and fostered the Internet as a free and open interoperable network of networks gave way to increasingly incompatible national and subnational legislation.

[35] The cases were authored using input gathered from five individuals who kindly presented 1) what they believed to be the key factors that will influence the future of the Internet and 2) their opinion on what the potential impact of these factors would be. We then drew upon this input to help write predetermined cases, namely what could be considered a best and worst case for Europe. The limitations of this approach is, like any scenario-planning exercise, the fact that the future is uncertain and will inevitably surprise us. We did not utilize any foresight instruments, scenario-planning methods, risk assessment tools or wider group consultations in their construction, thus limiting the diversity of perspectives in the formulation of the cases. Further, for consistency, the cases focus primarily on issues addressed in the previous chapters and only to a minimal extent include other key factors that will surely play a major role in the future of the Internet, including artificial intelligence, cyber warfare, augmented reality or other game-changing products and services, among other issues. The merit of this approach is to proactively think about the future and to use these cases as a means to either promote or prevent certain outcomes as opposed to only being reactionary in policymaking.

5. Conclusion and ideas for moving forward

In order to make progress towards achieving the best case and hedging against the worst case, the EU and European governments can take a number of steps with regards to protecting and advancing an updated vision of the free and open Internet underpinned by an effective and sustainable multistakeholder governance model. First, the EU and its member states need to defend and promote a strong and contemporary vision of the "free and open" Internet. A free and open Internet, balanced by appropriate regulation, remains the goal for which Europe and its like-minded partners should strive. In order to avoid an increasingly fragmented Internet on any layer, Europe needs to play a much more active diplomatic role promoting a clear narrative of how to achieve a balance between the ideal of a free and open Internet and the regulation needed to protect the rights of users, including protection of privacy and personal data.[36] While it is important that the EU should strengthen its ties with traditional partners such as the United States in order to promote the vision of a free and open Internet, these efforts would be particularly important in states sometimes referred to as "digital deciders" or "swing states", namely those countries that until now have remained largely apathetic about the future of the Internet, such as Brazil, Indonesia, Mexico and India, among others. Such states are subjectable to competing and repressive visions of Internet governance, for example, the authoritarian and government-driven models promoted by China and Russia.[37] Specifically, this could mean using its national delegations as well as EU member state delegations around the world as a clearinghouse for sensible Internet policies underscored by respect for human rights and consumer protection.

Further, the EU as well as member states should actively bring key issues of Internet governance into other relevant fora, for example, the G20, the Organisation for Economic Cooperation and Development (OECD) and other intergovernmental or multi-stakeholder convening processes at the national and international levels. For example, the EU should use its experience in adopting the General Data Protection Regulation to advocate for more harmonized international standards with respect to privacy and data protection across the world. At the same time, Europe should also look inward and ensure that its citizens reap the benefits of the European vision of the Internet and actively contribute to its positive evolution. In this respect, the EU and member states should drive efforts to, for example, promote digital literacy, strengthen democracy and government accountability through digital platforms for citizen engagement, and promote robust competition and innovation through the protection of non-discriminatory principles such as net neutrality.

Second, Europe should continue its strong support of the Internet Governance Forum by making it a more effective arena for decision-making on Internet governance issues.[38] One aspect of this is advocating for a more inclusive process, particularly through the enabling of participation from actors from developing countries or from those who otherwise lack the resources to bring their voices and concerns to the fore. More equitable access and wider participation can reinforce the benefits of the multi-stakeholder model and help ward off further attempts at the intergovernmentalization of Internet governance. Furthermore, European countries should work to turn the IGF into a premier arena not only for civil society, the technical community and working-level government officials, but also for the private sector – with a special focus on key players (digital champions) – and high-level political representatives through the promotion of new formats and processes for discussions. By sending its own representatives and encouraging their international counterparts to do the same, Europe can not only more effectively press its vision to other countries, but also garner greater international media attention to the importance of the IGF and the value of a free, open, secure and collaborative model of the Internet.

[36] Benner, T., Hohmann, M. (2018). *Getting „Free and Open" Right. How European Internet Foreign Policy Can Compete in a Fragmented World. GPPi Policy Paper.* Retrieved 15 February 2019, from https://www.gppi.net/media/Hohmann_Benner_2018_European_Internet_Foreign_Policy.pdf

[37] For more information on „digital deciders" and "swing states", see, e. g.: Morgus, R., Sherman, J. & Woolbright, J. (2018). *The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet.* Retrieved 14 June 2019, from https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/ & Maurer, T. & Morgus, R. (2014). *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate*. Retrieved 14 June 2019, from https://www.cigionline.org/sites/default/files/gcig_paper_no2.pdf.

[38] For a number of interesting ideas on how the IGF could be reformed, see e.g. United Nations (2019). The age of digital interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation. Retrieved 13 June 2019, from https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf.

6. References

B **Benkler, Y.** (2000). *From Consumers to Users: Shifting the Deeper Structures of Regulation Towards Sustainable Commons and User Access.* Federal Communications Law Journal: Vol. 52 : Iss. 3 , Article 9.

Benner, T., Hohmann, M. *(2018). Getting „Free and Open" Right. How European Internet Foreign Policy Can Compete in a Fragmented World.* GPPi Policy Paper. Retrieved 15 February 2019, from https://www.gppi.net/media/Hohmann_Benner_2018_European_Internet_Foreign_Policy.pdf.

Bygrave, L. A., Bing, J. (2009). *Internet Governance: Infrastructure and Institutions.* Oxford University Press.

C **Cerf, V. G. et al.** (1997). *Brief History of the Internet. Internet Society.* Retrieved 05 February 2019, from https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf.

D **Drake, W. Cerf, V., & Kleinwächter, W.** (2016). *Internet Fragmentation: An Overview.* Future of the Internet Initiative White Paper. World Economic Forum, January 2016. Retrieved 11 March 2019, from http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

G **Gross, R.** (2014). *Comments on Enhancing ICANN Accountability,* ICANN. Retrieved 11 March 2019, from http://forum.icann.org/lists/comments-enhancingaccountability-06may14/msg00036.html.

Gruber, B., Jaume-Palasí, L., Leidel, S., & Spielkamp, M. (eds.) (2016). *Guidebook Internet Governance: Media freedom in a connected world. DW Akademia.* Retrieved 18 March 2019, from https://www.dw.com/downloads/30373593/dwaguidebook-internet-governancefinal.pdf.

H **Hoxtell, W.** (2019). *The Web at 30: What's the State of Internet Governance?* Retrieved 14 March 2019, from https://www.gppi.net/2019/03/12/the-web-at-30.

I **ICANN** (2013). *Who Runs the Internet?* Retrieved 13 June 2019, from https://www.icann.org/en/system/files/files/governance-06feb13-en.pdf.

Internet Society (2019). *Internet Governance.* Retrieved on 14 February 2019, from https://www.internetsociety.org/issues/internet-governance/.

Internet Society (2019). *Open Internet Standards Chapter Toolkit.* Retrieved 18 March 2019, from https://www.internetsociety.org/chapters/resources/open-internet-standards-chapter-toolkit.

K **Kagan, R.** (2019). The strongmen strike back. The Washington Post. Retrieved 18 March 2019, from https://www.washingtonpost.com/news/opinions/wp/2019/03/14/feature/the-strongmen-strike-back/?utm_term=.53991c1517a5.

Kleinwächter, W. (2015). *The history of Internet Governance*, lecture at Summer Schools on Internet Governance. Retrieved 06 February 2019, from https://www.youtube.com/watch?v=5QUrkRtC2Js.

Kleinwächter, W. (2016). *Wer regiert das Internet? Internet Governance auf dem Prüfstand*. Vereinte Nationen 2/2016, p. 69. Retrieved 15 February 2019, from https://zeitschrift-vereinte-nationen.de/fileadmin/publications/PDFs/Zeitschrift_VN/VN_2016/Heft_2_2016/05_Beitrag_Kleinwaechter_VN_2-16_11-4-2016.pdf.

Kossow, N., & Webster, G. (2017). *The Pitfalls of Germany's New Hate Speech Law.* Transatlantic Digital Debates 2018 podcast. Retrieved 13 March 2019, from https://www.gppi.net/2017/07/19/the-pitfalls-of-germanys-new-hate-speech-law.

M **Maurer, T. & Morgus, R.** (2014). *Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate.* Retrieved 14 June 2019, from https://www.cigionline.org/sites/default/files/gcig_paper_no2.pdf.

Morgus, R., Woolbright, J. & Sherman, J. (2018). *The Digital Deciders – How a group of often overlooked countries could hold the keys to the future of the global internet.* New America report. Retrieved 20 March 2019, from https://www.newamerica.org/cybersecurity-initiative/reports/digital-deciders/.

N **Niesyto, J., Otto, P.** (2017). *Who governs the internet? Players and fields of action.* Retrieved 20 March 2019, from http://library.fes.de/pdf-files/akademie/13910.pdf.

S **Sacks, S.** (2018). *Beijing Wants to Rewrite the Rules of the Internet.* The Atlantic, 18 June 2018. Retrieved 01 March 2019, from https://www.theatlantic.com/international/archive/2018/06/zte-huawei-china-trump-trade-cyber/563033/.

Savage, J.E., and McConnell, B.W. (2015). *Exploring Multi-Stakeholder Internet Governance.* EastWest Institute, January 2015. Retrieved 11 March 2019, from https://www.files.ethz.ch/isn/188305/governance.pdf.

Spielkamp, M. (2016). *Internet governance – why we should care.* Interview for Deutsche Welle Akademie. Retrieved 20 March 2019, from https://www.dw.com/en/internet-governance-why-you-should-care/a-19320659.

U **United Nations** (2019). *The age of digital interdependence.* Report of the UN Secretary-General's High-level Panel on Digital Cooperation. Retrieved 13 June 2019, from https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf.

Unknown author (2016). *Understanding Media and Culture: An Introduction to Mass Communication. C*hapter 11.2: The Evolution of the Internet. University of Minnesota Libraries Publishing edition, available at https://open.lib.umn.edu/mediaandculture/.

V **Van Beijnum, I.** (2011). *25 years of IETF: setting standards without kings or votes.* ArsTechnica. Retrieved 18 March 2019, from https://arstechnica.com/tech-policy/2011/01/25-years-of-ietf-setting-standards-without-kings-or-votes/.

Vaughan-Nichols, S. J. (2019). *The EU's new copyright laws threaten to destroy the internet.* ZDNet Blog Networking. Retrieved 20 March 2019, from https://www.zdnet.com/article/the-eus-new-copyright-laws-threaten-to-destroy-the-internet/.

W **Working group on Internet Governance** (WGIG) (2005). *Report of the Working Group on Internet Governance,* Château de Bossey, June 2005. Retrieved 01 February 2019 at https://www.wgig.org/docs/WGIGREPORT.pdf.

Imprint

Published by:
Konrad-Adenauer-Stiftung e. V. 2019, Berlin

Image licensing: cover page, © unsplash/Markus Spiske
Design and typesetting: yellow too, Pasiek Horntrich GbR

Printed with financial support from the German Federal Government.

ISBN 978-3-95721-580-2

Konrad-Adenauer-Stiftung e. V.