Source: © Jason Lee, Reuters.

Multilateralism

Multilateral Approaches in Cyberspace

What is the Likelihood of an Internet Governance Regime?

Christina Bellmann

With increasing digitalisation, there is an increased need for internet regulation to protect human rights and democratic principles. Given the growing restrictions on the digital space imposed by authoritarian states, global efforts to protect the original free and open character of the internet, while counteracting fragmentation and restriction of fundamental rights, must be supported.

Since the invention of the internet, the digital space has invaded all areas of life and become an integral part of our daily routines. While, on the one hand, the internet has become a vital infrastructure, on the other hand, not enough is known about the political organisation of the internet on the multiple layers of the digital space.

The discussion about the structure and regulation of the internet has therefore shifted fundamentally in recent years: In addition to concerns about technical infrastructure, questions are increasingly arising concerning the rule of law, law enforcement, and the protection of human rights in the digital space. Given the global nature of the internet, these issues cannot be addressed exclusively at the national level but must be addressed globally. Unfortunately, the instruments of international law, which primarily regulate relations between states, are insufficient for the internet. As a decentralised network, the internet does not stop at national borders. The groups of players shaping the internet, such as telecommunications infrastructure providers, platform operators such as Amazon and Alibaba, and device manufacturers, are all much more diverse and heterogeneous than those in other multilateral regulatory regimes.

In order for the internet to remain a space and driver of innovation, exchange, and encounter, there must be increasing coordination and a broadened base of international law in the area of internet governance – i.e. a regime or regulatory system for the internet. The corona pandemic could reinforce this trend if areas that abruptly took place exclusively in the digital space – such as classroom instruction, large parts of the service sector, and administrative procedures – were to remain there in future. Germany should therefore expand its efforts to strengthen an internet governance regime based on liberal standards and values.

A Regime for the Internet

The last few years have seen numerous cases in which challenges caused by a lack of regulation of the internet were pointed out by whistleblowers. A prominent example was the global surveillance and espionage affair uncovered by Edward Snowden in 2013: The US' National Security Agency (NSA) and other security agencies broadly monitored telecommunications and parts of the internet, globally and irrespective of probable cause.[1] But discussions about the structure, functionalities, and leading players in this "network of networks"[2] still tend to take place in expert circles rather than in the general public.

The complexity of the internet means that conflicts cannot be clearly located on any given 'solution' level. These are global challenges that do not stop at national borders. For this reason, it is sensible to turn towards existing conflict resolution mechanisms in international organisations. However, not all relevant decision-makers, who are critical to shaping the internet, are present at the proverbial negotiating table – because most of the important ones are non-government players. Solutions to regulatory questions about the internet therefore

require a broader group of actors than is necessary for other multilateral, global challenges in the analogue world.

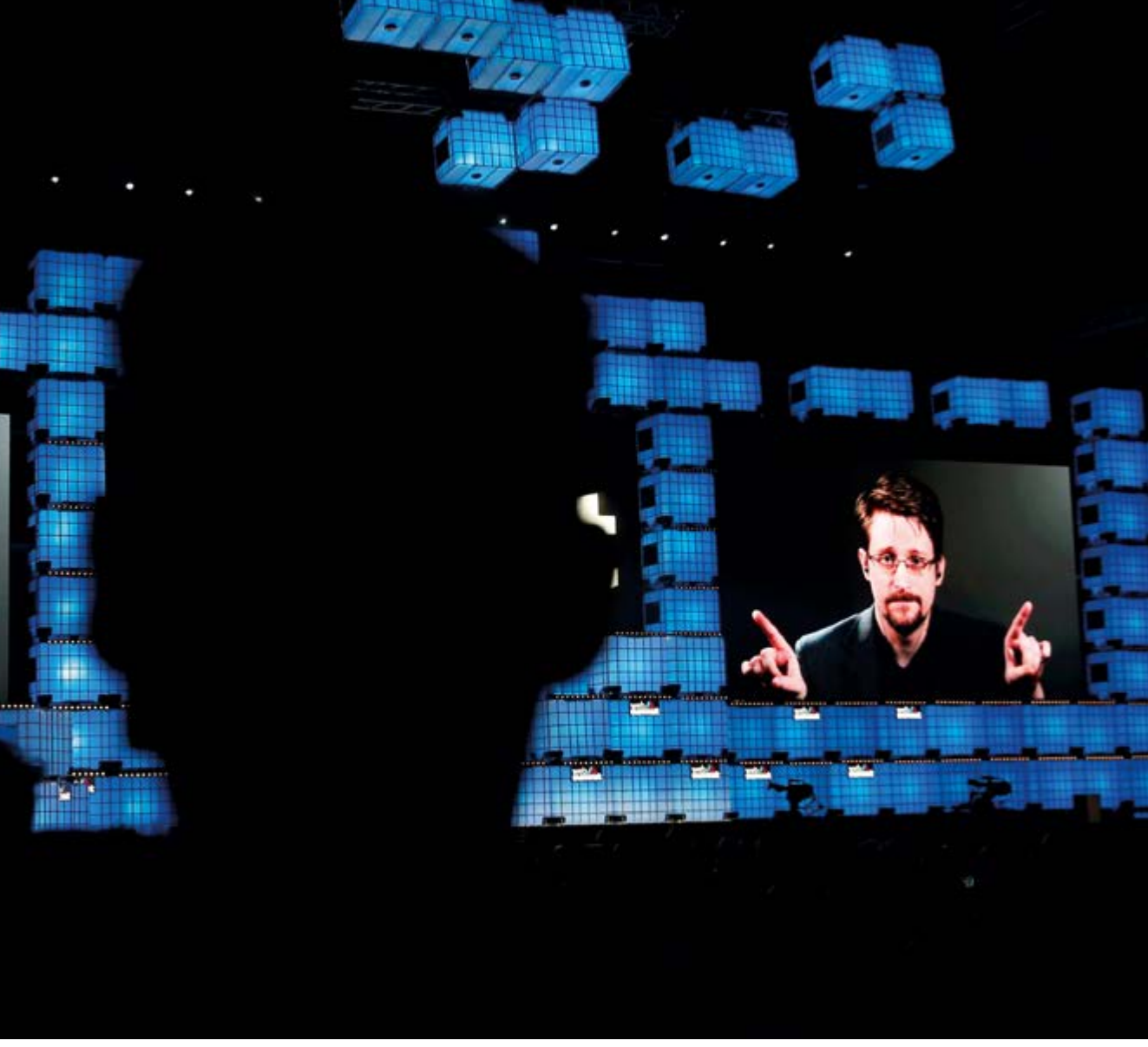
A look into science can help to rearrange our thinking about the complicated issue of internet governance: similarly complex problems, such as combatting global climate change and agreeing on fair global trade, are regarded in political science as "interdependence problems of a sectoral nature"[3]. Increasing globalisation has given rise to this analysis of regimes in international relations, a sub-discipline of political science. It explores sectoral interdependence problems and thus assesses "problems and conflicts in certain sub-areas of international relations (policy fields)"[4]. Regimes deal with conflicts between state and non-state actors (such as multinational corporations), as is the case, for instance, with climate change and global trade issues.

Challenges in these areas seem to be growing ever greater – partly due to the enormous complexity and magnitude of the problem fields – so that partial successes often go unnoticed in the media. However, it is difficult to prove post facto that, without agreements as part of a climate or global trade regime, similarly ambitious climate goals would nonetheless have been achieved or comparable economic value created.

This is the backdrop against which the demand arises for conflict resolution mechanisms and institutions as part of an internet governance regime, focussed on sustaining the system with all its advantages, while protecting democratic structures and achievements. A brief overview of the structure and foundations of the internet is thus helpful before delving into the complex question of regulatory options.

Structures and Organisation of the Internet – In the Beginning, there was Technical Coordination

The internet as we know it today was largely developed at the beginning of the 1990s.[5] The British physicist and computer scientist Tim Berners-Lee is considered to be its inventor. At the end of the 1980s, while working at CERN in Switzerland, he was looking for a way to exchange information between two independent university networks located in Switzerland and France. His solution to the problem enabled different existing networks to connect, allowing information to be exchanged through a global electronic communications network. The open structure and free access to the internet protocols thus created, enabled the network to grow quickly and to integrate a vast array of networks all over the world.



Controversial voice: The last few years have seen numerous cases in which challenges caused by a lack of regulation of the internet were pointed out by whistleblowers. Source: © Rafael Marchante, Reuters.

Simply put, the internet consists of different layers, of which the lowest is the physical infrastructure (cables and electromagnetic waves to transfer data).[6] Above that is the middle layer of internet protocols, which ensures data transfer between sender and receiver through interfaces. The top layer is the one the user perceives: applications, web pages, and e-mail programmes.

The first regulatory institutions relevant to the internet were essentially concerned with the lowest layer and with the technical standards of its functionality. In so doing, they were following the development path laid out by earlier communications technologies, such as radio or telephone; in some cases, they emanated from the same structures or were integrated into them. For instance, one of the earliest special United Nations organisations with a mandate to coordinate global technical standards is the International Telecommunication Union (ITU).[7] Originally founded in 1865 with the aim of connecting existing international telegraph networks, it laid the groundwork for much of the

standardisation in the area of telecommunications and wireless communications that is still used today. Today, it has 193 member states.

One of the first institutions to focus solely on the internet, the Internet Assigned Numbers Authority (IANA), founded in 1988, concerned itself, simply put, with assigning IP addresses – i.e. the middle layer.[8] Later, it was integrated into the Internet Corporation for Assigned Names and Numbers (ICANN), founded in 1998. ICANN has the task of coordinating the central register for assigning unique names and addresses on the internet.[9] Unlike the ITU with its UN member states, ICANN was founded as a private-sector regulatory authority by the US government under the Clinton administration with the participation of executives from leading US information technology corporations of the time, such as IBM and AOL. It was set up with the intent to counteract the international patchwork of national standards and bodies of legislation. From today's perspective, it may seem paradoxical that the leading telecommunications corporations of the 1990s supported an international organisational regime outside of the ITU, but it suited the neoliberalism of the US at the time and its aversion to state and interstate bureaucracy and to the long negotiation processes involved in the UN system.

There was state resistance to the ICANN's founding motivated by fear of having no influence on important decisions.

ICANN was thus an US-dominated authority that was intended to be completely privatised and made independent within two years. But this step kept being postponed because of US' interests. As long as there were only a few players in the internet and the organisation was functioning, ICANN's position went relatively undisputed, and there was little reason to change the existing system. In addition to IANA and ICANN, a number of other technical coordination institutions arose, following the approach of a free, open multi-stakeholder internet – an internet that was formed by many different participants – and thus advocated for as little state regulation as possible.[10] This approach – a free, open internet outside of state-dominated institutions such as the UN – contributed to the internet's unprecedented global development. Effective technical coordination underpinned ICANN's long record of success, and its legitimacy was not questioned at first. Most private players had no interest in changing the system as long as telephone numbers and IP addresses were assigned in a manner which worked.

From "Free and Open to All" to More State Participation

From the very beginning, there was state resistance to ICANN's founding: Motivated by the fear of insufficient influence over important ICANN decisions, a number of European governments advocated for the involvement of governments and international institutions. That is why the Governmental Advisory Committee (GAC) was added to the ICANN structure. At the first World Summit on the Information Society (WSIS) in 2003, China, Brazil, Russia, South Africa, and a number of developing countries, with the support of the ITU, expressed criticism of the current internet governance structure. A conflict arose between two camps: On the one hand, there were states and actors, which criticised US dominance in the current decision-making system and wanted a multilateral institution, representatives of the private sector, the US, and other organisations, on the other hand, supported the status quo and dismissed the necessity of governance structures for the internet.

The result of the WSIS was the founding of the Working Group on Internet Governance (WGIG), which had a variety of tasks, including developing a working definition of internet governance, identifying public policy issues

involving the internet, and listing internet stakeholders and their roles and responsibilities.

The WGIG contributed to the establishment of a broader understanding of internet governance, defining it as "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 use of the Internet".[11]

The Working Group's primary proposal was the foundation of a new multi-stakeholder forum to tackle internet-related issues.

This gave rise, in 2005, to the Internet Governance Forum (IGF), whose participants can be roughly divided into four stakeholder groups: states, private corporations, civil society groups, and the so-called "epistemic community" made up of technical experts.[12]

Control of technical hubs and standards can allow authoritarian governments to abuse their power and limit democratic rights.

This is where the transition from technocratic cooperation issues to a broad concept of internet governance, with increasingly complex coordination issues, becomes clear. The interests of the "epistemic community" are associated with the interests of businesses[13] whose future profitability depends on future internet standards. Nonetheless, these technical and economic matters should not distract from the fact that conserving standards and laws on the internet, protecting human rights, as well as free access to the network is becoming increasingly important. That is why the two spheres can no longer be viewed independently from one another: limits to technical infrastructure can lead to the formation of monopolies or oligopolies and to the distortion of opportunities to the detriment of smaller companies and start-ups. Moreover, control of technical hubs and standards, such as the new 5G technology, can lead to abuse of power by authoritarian governments and to restrictions on the democratic rights of societies. All these issues should be discussed within the framework of the Internet Governance Forum so that the widest possible consensus can be reached on the further development of the internet. These are high expectations of a single forum, and critics allege that it is too self-referential and insufficiently output-oriented.

New Challenges – E-currencies, IoT, AI, and Corona

The speed of technological change has had a significant impact on societal life and led to generations of digital natives and digital immigrants living together in a quickly-changing, media-driven world.[14] The internet contributes to the formation of public opinion, influences how policy is made, and how states communicate with one another. Technical disputes about details such as the availability of domains or IP addresses in the current internet protocol or the transition from the IPv4 to the IPv6 system are juxtaposed with questions of data protection and human dignity.

A few examples show how new technologies have the potential to fundamentally change existing governance systems:

E-currencies

Digital currencies developed by commercial companies challenge the current system, which is based on state actors and central banks. Potential benefits, such as transparency, security, and efficiency due to blockchain technology, are countered by issues of standard setting, system security, and stability.[15] Cryptocurrencies already play a decisive role in the fight against terrorism and organised crime: diverging international standards with regard to the freezing or confiscation of funds to finance illegal activities make regulation difficult. For cryptocurrencies

to be useful, they must be converted into existing currencies. This is the opportunity for prosecution. The increasing opportunities for using cryptocurrencies outside the state-regulated banking system could become a problem for law enforcement and thus a challenge for an important pillar of democratic systems.

Autonomous Driving

Autonomous vehicles are, so to speak, data centres on wheels,[16] with hardware, software, sensors, etc. The advantages of automated vehicles are similarly balanced by the risks of hacker attacks – which could affect not only street traffic, endangering human lives, but also gain access to car manufacturers' corporate networks using compromised vehicles.

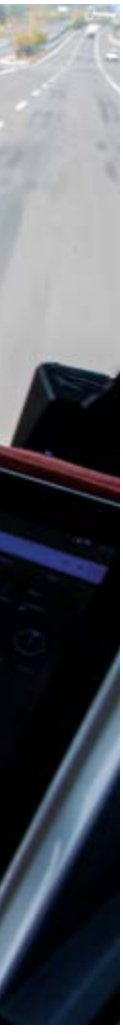
Protecting Privacy – Internet of Things (IoT) and AI

The mass collection of personal data in so-called smart home hubs is not the result of hacking, but rather the raison d'être of these systems, enhancing their functionality.[17] Many of these smart household devices communicate not only with their manufacturers, but also

Risk and opportunity at once: The advantages of automated vehicles are similarly balanced by the risks of hacker attacks. Source: © Thomas Peter, Reuters.

with third parties, in some cases without the user's knowledge or consent. Due to the transnational activities of appliance manufacturers, various national legal systems come into play. The national differences in areas such as evidence law make it harder to reach an agreement on how manufacturers and information providers should store data collected from IoT devices.

As a result, crucial processes of our democracies are rendered even more vulnerable to direct digital attacks.



The corona pandemic has also (at least temporarily) further accelerated this development: social distancing requirements make digital networks even more important than before and internet-based services via platforms such as Amazon and Netflix are growing at an unprecedented rate.[18] Providers of video technology, such as Zoom and Microsoft, are experiencing rapid sales and, in some countries, parts of court proceedings are performed by videoconference.[19] Large parts of national and international parliamentary work was shifted to the internet. For instance, Germany's Bundestag and the European Parliament hold many of their sessions online in order to remain functional while maintaining the social distancing. As a result, crucial processes of our democracies are rendered even more vulnerable to direct digital attacks, from disruptions aimed at impeding work to theft of confidential documents by hackers.

Climate Regime, World Economic Regime, Internet Regime?

All these examples show that the need for cooperation in the area of internet governance is growing and that much thought must be given to new conflict resolution mechanisms. The integration of various sectors in the area of the internet is further complicated by the large number of actors involved. The history of multilateral regimes shows that without them, actors, which behave cooperatively, are at risk of being exploited by those that do not. This has been seen in regimes to govern global trade relations – i.e., the global currency regime with the IMF and others, the global trade regime with the GATT and the WTO, or the development regime with the World Bank group – and with the climate regime. The internet will be no different. Put bluntly, if there is no agreement on the further development of the internet, the entire system is at stake.

Previous international regimes were limited in their scope in one manner or other: global trade regimes are currently largely based on decisions made by nation states and central banks. Although the climate regime is viewed globally, it is regulated and implemented at the regional or local level – albeit with a few exceptions, such as emissions trading. The human rights regime is anchored in international law but implemented by national executives. There are no such limits to the internet.

An additional concern with the issue of internet governance is that, as outlined above, we are dealing with a complicated ensemble involving a growing number of policy areas, which must all be taken into consideration. The intricacy of these various policy areas, their level of interconnectedness, and the variety of organisation and personnel involved, not all of whom are organised within the existing regime, make negotiations about internet governance unbelievably difficult. This complexity is well known, which is why the Internet Governance Forum should be adapted and further developed, accordingly.

Multi-Stakeholder Initiatives vs. Internet Multilateralism

By signing Tim Berners-Lee's "Contract for the Web",[20] presented at the 2019 Internet Governance Forum in Berlin, the German federal government expressed its support for an ambitious initiative that will bring an internet governance regime one step closer. The "Contract

Building trust: platforms such as the Internet Governance Forum promote a free, open, liberal internet.
Source: © Ludovic Marin, Reuters.

for the Web" obligates governments, companies, and civil society to support the basic idea of the internet for the future. Each of the signatory groups in this multi-stakeholder initiative has a different obligation to fulfil. States are to ensure internet access for all, prevent the network from being blocked, and ensure data protection and basic digital rights. Companies are obligated to make the internet affordable and accessible, to respect privacy and human rights, and to develop open technologies that prioritise users over profit. Civil society is to cooperate for the further development of the internet, facilitate strong discourse that supports human dignity, and promote a free, open, liberal internet.

The initiative thus takes up the four-pronged structure that Harald Müller, a political scientist and leading regime theoretician, believes is necessary for establishing a regime: principles, standards, rules, and decision-making procedures.[21] It also integrates all the relevant stakeholder groups identified above into a joint consultation process. It considers both the technical cooperation component and the fundamental rights that people in the analogue world enjoy.

From a theoretical perspective, this seems like a good starting point for the successful establishment of an internet regime. Müller notes that

success requires cooperation, which takes place over a longer period of time, allowing the players to develop the necessary trust in the regime's effectiveness.

The German federal government provides state support within the framework of the Alliance for Multilateralism. This informal alliance was created in April 2019 by countries "united in their conviction that a rules-based multilateral order is the only reliable guarantee for international stability and peace and that our common challenges can only be solved through cooperation".[22] One of the alliance's initiatives is the Paris Call for Trust and Security in Cyberspace.[23] Those engaging in such calls for a multilateral internet governance regime, however, must take care not to use the same language as that used for different demands. At the 2014 Shanghai Cooperation Organisation, for instance, China and other states called for an internet governance system of "multilateralism, democracy, and transparency" and a "cyberspace of peace, security, openness, and cooperation".[24] This lip service to multilateral principles must not distract from the fact that states such as Russia and China call for more state sovereignty in the area of the internet in order to become gatekeepers for their populations' access to certain areas of the internet. By separating national networks, they also contribute to the fragmentation of the internet.

Opportunities for an Internet Governance Regime

In light of the many different players and the already existing fragmentation of the internet, it seems naive to call for global initiatives to regulate this complex space. Moreover, despite their long histories, other regimes for enforcing global environmental, trade, or human rights standards have shown only mixed success in tackling complex problems. Nevertheless, given the omnipresence of digital changes, it appears necessary to consider promising initiatives for an internet governance regime. Increasing digitalisation of communications requires protections for freedom of speech, the press, assembly, and privacy on the internet just as in analogue life. These freedoms are essential to the functioning of democracies and are increasingly under pressure from authoritarian states, which are restricting more and more fundamental rights in the digital space.

Far-reaching effects on our daily lives make it all the more urgent that initiatives such as the Internet Governance Forum be supported and considered in conjunction with all areas of policy. It is important that as broad a consensus as possible is found among like-minded states, corporations, civil society groups, and scientists so as to counteract authoritarian tendencies. Discussions of the supposedly technical issues must not disguise the fact that the further development of the internet involves decisions with far-reaching political implications. Multilateral structures and institutions must take the multi-stakeholder structure of the internet into account if they are to achieve a balance between having a free and open space for innovation and protecting fundamental rights.

–translated from German–

Christina Bellmann is Policy Advisor for European Affairs / Multilateral Dialogue at the Konrad-Adenauer-Stiftung.

1 Beuth, Patrick 2013: Alles Wichtige zum NSA-Skandal, ZEIT Online, 28 Oct 2013, in: https://bit.ly/3kMeamQ [10 Aug 2020].
2 Weise, Sebastian 2019: World Wide Web oder doch Wild Wild West?, Konrad-Adenauer-Stiftung, 12 Mar 2019, in: https://bit.ly/3h8ek5K [1 Jun 2020].
3 Zürn, Michael 1992: Interesse und Institutionen in der internationalen Politik: Grundlegung und Anwendung des situationsstrukturellen Ansatzes, Opladen.
4 Ibid.
5 World Wide Web Foundation 2020: History of the Web, in: https://bit.ly/3iJjWEf [9 Aug 2020].
6 Hohmann, Mirko / Benner, Thorsten 2018: Getting "Free and Open" Right: How European Internet Foreign Policy Can Compete in a Fragmented World, Global Public Policy Institute (GPPi), Jun 2018, in: https://bit.ly/31S29Uw [9 Aug 2020].
7 International Telecommunication Union (ITU) 2020: About International Telecommunication Union, in: https://bit.ly/33XyJHd [1 Jun 2020].
8 Digital Guide Ionos 2019: IANA: Verwaltungseinheit des Internets, 21 Jun 2019, in: https://bit.ly/3ixLQTw [1 Jun 2020].
9 Mueller, Milton / Mathiason, John / Klein, Hans 2007: The Internet and Global Governance: Principles and Norms for a New Regime, Global Governance 13: 2, pp. 237–254, in: https://bit.ly/3azRqBR [18 Aug 2020].
10 For a short overview of the history of internet governance and the institutions and players that largely shape the internet today, see: Hoxtell, Wade / Nonhoff, David 2019: Internet Governance: Past, Present, and Future, GPPi, 22 Nov 2019, in: https://bit.ly/2PSVx2A [10 Aug 2020].
11 United Nations Department of Economic and Social Affairs 2005: What is Internet Governance?, in: https://bit.ly/3gW7Vup [9 Aug 2020].
12 An, Jungbae/ Yoo, In Tae 2019: Internet Governance Regimes by Epistemic Community – Formation and Diffusion in Asia, Global Governance 25: 1, pp.123–148.
13 Ibid.
14 More information about how digital media affect social processes can be found in a systematic 1990s study on mediatisation, conducted during the quick proliferation of such media, see: Krotz, Friedrich 2010: Mediatisierte Welten – ein Schwerpunktprogramm (SPP) der DFG, in: https://bit.ly/3fTgCV3 [1 Jun 2020].
15 Chumtong, Jason 2020: Digital Money for the Digital State, in: International Reports 36: 1, Mar 2020, in: https://bit.ly/2FwQfrv [20 Aug 2020].
16 Rähm, Jan 2020: Hacker an Bord: Fachleute besorgt um IT-Sicherheit vernetzter Pkw, Deutschlandfunk, Forschung aktuell, 29 May 2020, in: https://bit.ly/3gRf1At [10 Aug 2020].
17 Rens, Andrew 2019: Who is in Charge Here? The Internet of Things, Governance and the Global Intellectual Property Regime, in: UCLA Journal of Law & Technology 23: 2, in: https://bit.ly/3hraIvO [20 Aug 2020].
18 Barkhausen, Barbara 2020: Corona verhilft Netflix zu gewaltigem Nutzerzuwachs, Gründerszene, 22 Apr 2020, in: https://bit.ly/31PUpCv [10 Aug 2020].
19 Law, Paulitsch 2020: Der Einsatz von Videotechnologie im Gerichtssaal – neue Regeln zu Videokonferenzen in zivilgerichtlichen Verfahren, Linde Media, 7 May 2020, in: https://bit.ly/31T4Nt0 [10 Aug 2020].
20 Contract for the Web 2019: Contract for the Web – A global plan of action to make our online world safe and empowering for everyone, in: https://bit.ly/30VnVYd [1 Jun 2020].
21 Müller, Harald 1993: Die Chance der Kooperation: Regime in den internationalen Beziehungen, Darmstadt, p. 26.
22 Ministère de l'Europe et des Affaires étrangères 2019: Allianz für den Multilateralismus, in: https://bit.ly/3iDcNoP [1 Jun 2020].
23 Federal Foreign Office 2019: Six initiatives for multilateralism, 26 Sep 2019, in: https://auswaertiges-amt.de/en/2250460 [25 Aug 2020].
24 Bradshaw, Samantha / DeNardis, Laura / Hampson, Fen Osler / Jardine, Eric / Raymond, Marc 2015: The Emergence of Contention in Global Internet Governance, CIGI Paper Series 17, Centre for International Governance Innovation (CIGI) / Chatham House, in: https://bit.ly/31QGMmj [14 Aug 2020].