Infrastructuring Cyberspace: Exploring China's Imaginary and Practices of Selective Connectivity

Huang, Ying; Huppenbauer, Nicolas; Mayer, Maximilian

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Huang, Y., Huppenbauer, N., & Mayer, M. (2022). Infrastructuring Cyberspace: Exploring China's Imaginary and Practices of Selective Connectivity. *International Quarterly for Asian Studies (IQAS)*, *53*(3), 413-439. https://doi.org/10.11588/iqas.2022.3.13947

IQAS Vol. 53 / 2022 III, pp. 413–439

Infrastructuring Cyberspace
Exploring China's Imaginary and Practices of Selective Connectivity

Ying Huang, Nicolas Huppenbauer, Maximilian Mayer

Abstract

Connectivity and fragmentation coexist as two interlinked discourses on the relationship between infrastructures and societies. In response to the Digital Silk Road initiated by the Chinese government, Chinese companies have built numerous digital infrastructures globally. Simultaneously, China's government seeks to strengthen domestic internet governance through laws and administrative regulations, such as the Cyber Security Law. This paper utilises the interpretive framework of "sociotechnical imaginaries" to explore the controversial tension between digital fragmentations and connectivity in cyberspace along technical, institutional and political dimensions. Scrutinising two cases studies – New IP and smart city – the study finds that China's approach to infrastructuring cyberspace can be best understood as selective connectivity. China not only integrates into global cyber infrastructures to enhance its technological and regulatory capabilities, but also attempts to reshape global cyberspace governance to strengthen its political structures and enhance digital autonomy, seeking a balance between digital sovereignty, regime security and economic development. However, selective connectivity brings its own complexities and drawbacks.

Keywords: China, New IP, smart city, connectivity, cyberspace, sociotechnical imaginaries

Ying Huang, Institute of European Studies, Chinese Academy of Social Sciences, Beijing, China; yinghuang@cass.org.cn. Nicolas Huppenbauer, Center for Advanced Security, Strategic and Integration Studies, University of Bonn, Bonn, Germany; nicolas.huppenbauer@uni-bonn.de. Maximilian Mayer, Center for Advanced Security, Strategic and Integration Studies, University of Bonn, Bonn, Germany; maximilian.mayer@uni-bonn.de. The authors' research for this article has been funded by the Returning Scholars Program of the Ministry of Culture and Science of the State of North Rhine-Westphalia, Germany (research group "Infrastructures of China's Modernity and their Global Constitutive Effects"); the China Postdoctoral Science Foundation Special Funded Project "Digital Fragmentation from the Perspective of Global Digital Sovereignty" (grant no. 2022T150722), and the Postdoctoral Innovation Program of the Chinese Academy of Social Sciences. The authors would like to thank the anonymous reviewers and the journal editors for helpful comments and suggestions.

DOI 10.11588/iqas.2022.3.13947

> Across the Great Wall, we can reach every corner of the world.[1]

Introduction

Cyberspace is under reconstruction.[2] Global digital infrastructures – an integral part of globalisation enabling cross-border interactions and creating multi-layered interdependencies – have come under growing pressure. Restrictions, interventions and boundaries are multiplying in a realm that was once envisioned as borderless, popularised through notions such as "global village" and "network society". Ultimately global in their reach by nature, digital infrastructures embody the idea of ubiquitous connectivity. They are also, however, crucial sites where major technopolitical reconfigurations can be observed (Munn 2020).

As a quintessential "infrastructural state" (Bach 2016, Schindler et al. 2022, Ho 2020), China is perceived by many as the main agent that aims at reshaping cyberspace in its own image. Chinese actors are seen as both ideational promoters and technical engineers of data nationalism, cyber sovereignty and digital authoritarianism, thereby splintering the internet (Deibert et al. 2010, Diamond 2019). To grasp the ways in which the Chinese government and firms are indeed reshaping cyberspace is therefore a highly relevant yet complex issue. Two conflicting approaches can be observed: China emphasises cyber sovereignty for the sake of domestic stability and technological autonomy (Segal 2020) and maintains the Great Firewall that partially disconnects more than a billion internet users in China from global communication flows. Simultaneously, the Chinese President Xi Jinping publicly defends globalisation and advances the technical integration of global networks, as Chinese companies construct optical cables, satellites and other communication networks and software platforms to improve local, inter-regional and planetary connectivity.

This complexity indicates the salience of the scholarship on balkanisation, splinternet and islandisation and complicates this research subject at the same time. To empirically and conceptually capture the dynamics of the emerging technopolitical reality of digital "fragmentation" (Malcomson 2016, Mueller 2020) requires nuance. While some focus on the reinforcement of national jurisdictions as the main culprit (Drezner 2004, Mueller 2017), others distinguish between technical, governmental and commercial fragmentation (Drake et al.

1 From the first email sent via CSNET from the Beijing Institute for Computer Application of State Commission of Machine Industry, China, to the Karlsruhe Institute of Technology, Germany, on 14 September 1987.

2 Cyberspace can be defined as "a global domain [...] framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies" (Kuehl 2009: 28).

2016) and identify diverse actors and processes that produce fragmentation (Hill 2012). A binary distinction tends to underpin views on Chinese cyber policies, dividing approaches to cyber governance into democratic and authoritarian (Hoffmann et al. 2020). To go beyond such a reductionist view and to avoid the trap of "digital orientalism" (Mayer 2020, Mahoney 2022), we argue that the inherent complexity of China's bearing on global cyberspace governance requires a conceptual approach that captures the current blending of digital fragmentation and connectivity. For that purpose, two empirical questions guide our research: What kind of imaginary of connectivity animates Chinese practices of infrastructuring cyberspace? And what are the outcomes of employing this imaginary while building digital infrastructure abroad?

The paper employs the interpretive framework of "sociotechnical imaginaries" (Jasanoff / Kim 2015) to explore China's vision and practices concerning cyberspace in a broader social, economic and political context. Understanding infrastructure as an activity – *infrastructuring* – shifts the focus from a supposedly stable system to the practices needed to create and maintain or enlarge them further (Korn et al. 2019, Star / Ruhleder 1996). We explore how social and political contexts shape sociotechnical imaginaries of connectivity in China and how, in turn, the involvement of Chinese tech companies in the build-up of infrastructures changes global connectivity (Shen 2021). By analysing two digital infrastructures in the making, specific practices of fragmentation / connectivity ranging from the local to the global scale are scrutinised.

We analyse, firstly, the public controversies around the "New IP" proposal, a Chinese initiative at the International Telecommunication Union (ITU). Various organisations and commenters have claimed that New IP would not only harm interoperability in cyberspace, but also potentially make internet censorship and data regulation more convenient (IETF 2020). Secondly, we investigate the "Smart City Duisburg" in Germany, where Huawei's involvement attracted international attention. Based on the analysis of press releases, interviews and policy documents, we trace Huawei's impact on interoperability and internet governance norms at the nexus of digital urban transformation and contestations over transparency and participation.

In the following section, we lay out the key concerns with connectivity and fragmentation. In the third section, we introduce the framework of sociotechnical imaginaries and demonstrate its general applicability to exploring China's practices of infrastructuring cyberspace. In the fourth section, we examine two case studies – "New IP" and "the Smart City Duisburg" – in light of China's imaginary of selective connectivity. The fifth section discusses the main lessons from the two case studies. We conclude by reflecting on the notion of selective connectivity.

Connectivity and fragmentation in cyberspace

Connectivity and fragmentation coexist as two powerful and interlinked discourses on the relationship between infrastructures and societies. The notion that infrastructures should facilitate the circulation of goods, people and information has been an influential discourse since at least the 17th century (Mattelart 2000, van der Vleuten 2004: 396–399).[3] In 1841, Friedrich List lamented in his *National System of Political Economy* that a lack of railway connections would impede unification of the scattered German states (List 1885). Deepened global connectivity has been at the root of discussions about globalisation, while various large technical systems became the backbone of modern international relations (Mayer / Acuto 2015). Andrew Giddens claims that modernity was "inherently globalising", leading to the "intensification of worldwide social relations" (Giddens 1990: 63).

Building on Giddens, John Tomlinson argues that connectivity implies sociocultural proximity: "connectivity means changing the nature of localities and not just occasionally lifting some people out of them" (Tomlinson 1999). Manuel Castells's influential notion of "network society" was derived from the observation that the rise of global information and communication networks had induced a historic transformation of human existence, allowing for a change in practices of organising (Castells 2010). In addition, connectivity has become a buzzword among policy-makers and business elites. For example, the Association for Southeast Asian Nations (ASEAN) has for over a decade put connectivity at the heart of its Master Plan:

> Connectivity in ASEAN refers to the physical, institutional and people-to-people linkages that comprise the foundational support and facilitative means to achieve the economic, political-security and sociocultural pillars towards realising the vision of an integrated ASEAN Community (ASEAN 2011: 8).

A report by the global management consulting firm McKinsey highlights the significance of connectivity for industrial applications such as the Internet of Things[4] (Alsen et al. 2017), while the World Bank Group (2019) regards connectivity as a distinctive feature of the modern economy and a major trend in the 21st century. Godehardt and Kohlenberg (2020) argue that the narratives and proposals around the BRI have been a major promoter of this spatialised discourse of globalising geoeconomics.

The concern with the fragmentation of the internet, however, is increasingly taking centre stage. The problem of the internet's "splintering or breaking up into loosely coupled islands of connectivity" (Drake et al. 2016: 3) is not new.

3 See Edwards (2003) on the link between infrastructures and modernity.

4 "Internet of Things", abbreviated as IoT, refers to the network of sensor-equipped and interconnected objects, such as streetlights, cars and house appliances.

Even before the global expansion of the internet, in 1991, Al Gore called for the prevention of a splintering of the emerging cyberspace by establishing common standards and technologies (Gore 1991). Internet fragmentation was constitutive to the creation of the internet from the beginning, it occurred in the technological as well as in the governmental and commercial domains (Herrera 2002, Mueller 2010, Drake et al. 2016).

After the Snowden revelations in 2013, the idea that states should intentionally produce fragmentation gained legitimacy: advocates of "data localisation" demanded that data storage, movement and processing be organised within their jurisdictional borders (Hill 2014). Cyber borders also became a positive idea more broadly connected to resurging populism (Cox 2017) and strongly linked with ideas of sovereignty and a resurgence of national interests (Nussbaum 2010, Paris 2020). The prominence of ideas such as "decoupling" and the US Clean Network initiative indicates that disconnectivity is not only an issue limited to China: "the United States has been deploying a multi-faceted campaign since the Trump administration that combines persuasion, coercion and incentives to dissuade Washington's allies from accepting projects involving Chinese suppliers" (Velliet 2022: 21).

For instance, the European Union's "Global Gateway", set out on 1 December 2021, is seen as the European alternative to China's Belt and Road Initiative (BRI). Policy makers and the public at large, it seems, are progressively developing the sense that globalisation is undergoing a significant transformation, calling into question the goal of ever-deepening connectivity (Fontaine 2020, Lund et al. 2019). This shift of thinking about connectivity is reflected in the new theorisation of interdependence and its weaponisation (Drezner et al. 2021, Farrell / Newman 2019, Keohane / Nye 2012). Observers point out that various states have begun to instrumentalise economic flows and interactions, thereby giving rise to a "connectivity war" (Leonard 2016). Connectivity infrastructures are conceptualised as subject to great power competition.

China's imaginary of selective connectivity

China's approach to connectivity is ambiguous. It can best be described as selective: on the one hand, China's integration into cyberspace has continually grown since 1987, when the first email from China was sent abroad. In 1995, the country set up its first commercial internet connection (Choy / Cullen 1999: 105). According to official estimates, China had 1.032 billion internet users in 2021 (Global Times 2022). In 2019, the Chinese mainland together with Hong Kong had cross-border data flows of 111 million Mbps, accounting for 23 per cent of global data flows (Nikkei 2020). The country's techno-political strategies

such as the Digital Silk Road (DSR), China Standards 2035 and New Infrastructure represent initiatives to further connect the country domestically and globally.

On the other hand, the establishment of a legal and regulatory frameworks to control information flows and enable greater technological autonomy has emerged as one of China's key priorities. Since the origins of the internet in China, the government has constructed and updated the Great Firewall. This infrastructure functions to selectively block access to foreign websites and communication, which seems to contradict the purported focus on connectivity (Barme / Ye 1997). Moreover, since the 2010s, there is an emerging consensus among Chinese political and economic elites that digital technology can not only help China to withstand a variety of economic and social troubles, but even be applied as a tool to enhance the functions and stability of the Chinese political system (Creemers 2020: 113, Huang / Tsai 2022). In sum, China seeks to continuously strengthen technical and commercial connections with and through the global cyberspace, but wants to partially reduce the influence of western values, shielding its institutional and socio-cultural norms. The emphasis on mitigating technical and economic interdependencies seems to counteract the bid by Chinese tech firms to develop greater influence in global cyberspace (Mayer / Huotari 2015, Huang / Mayer 2022).

As reflected in China's practices of infrastructuring its internal cyberspace, a mix of connectivity and fragmentation characterises the Chinese sociotechnical imaginary. The concept of "sociotechnical imaginaries" (STI) was first introduced by Sheila Jasanoff and Sang-Hyun Kim (2009) in order to explain the relationship of science and technology to political power. STIs are "collectively held, institutionally stabilized, and publicly performed visions of desirable futures, animated by shared understandings of forms of social life and social order attainable through, and supportive of, advances in science and technology" (Jasanoff 2015: 4). STIs have been employed to study which features of national political culture are embedded in the development and expectations of science and technology and, thus, how technoscientific and political orders are coproduced. We draw on the insights of earlier work. While STIs have been used to explore cyberspace as coproducing freedom (Barker 2015), democracy (Felt 2015) and citizenship (Isin / Ruppert 2020), the framework also offers a way to investigate infrastructuring practices and connectivity in both democratic and authoritarian environments.

Imaginaries are widely reproduced by collective thinking and reflected in national decision-making. STIs can be traced in the meaning that is transported by acts of speech and performance, and by acts of stabilisation, such as the foundation of new institutions and organisations, the drafting of legal texts and policy documents, the launching of hallmark strategies and initiatives, and the construction of material infrastructures. Scholars point out that Chinese

policies and emerging sociotechnical systems reflect negotiations between various actors within the Chinese government, but also from industry and civil society (Shen H. 2016). Notable examples include cases such as the Hainan provincial government seeking an exemption from the comprehensive online censorship regime (Lu 2020) and disputes among consumers, firms and the government over the neutrality of Chinese telecommunications and service providers (Murphy / Qian 2021, Wu / Wan 2014).

Despite a variety of actors and interests in the Chinese context, it is possible to distinguish some broad directions of the Chinese policy-industry-society nexus (Cai / Dai 2021). The key question is not whether an STI determines the outcomes of all of China's actions on cyberspace, but rather whether it shapes and is reproduced by practices across various societal sectors and points in time. Moreover, the Chinese government is a powerful actor that seeks to push through its vision, for example by allocating funds in a certain way, and that can actively influence which visions are collectively adopted and maintained (cf. Jasanoff / Kim 2009). For example, Hong Yu (2017), though stressing the diverging interests of Chinese organisational actors in the creation of nationwide telecommunications infrastructures, acknowledges that they may still imagine a similar destination for China as a country.

In the 1990s, Chinese elites were generally receptive to US demands for a more open telecommunications sector. Their approach to partially adopting rules and structures of global digital capitalism was shaped by the country's experience of introducing market reforms in the communications sector while trying to avoid the neoliberal failures observed in the West. As China was preparing to join the WTO in 2001, competing views and objectives within the Chinese government and between the state and industry persisted. But the aspiration to integrate into and eventually to shape global information infrastructures nonetheless led to a common vision for both state and business (Hong 2017: 150–153). Samuel Lengen argues that the convergence of Chinese government and industry narratives on the promises of digital connectivity for the Chinese nation would not have been achieved without the daily experiences and contributions of Chinese citizens. The everyday use of Alibaba's digital platforms by Chinese from all over the country, he suggests, made the company a symbol of national pride and of China's international competitiveness (Lengen 2022).

In the following, we focus on two practices to illustrate the sociotechnical imaginary of selective connectivity: institutionalisation and public performance.

Institutionalising cyber sovereignty

> [Institutions are] stable repositories of knowledge and power […] through which the validity of new knowledge can be accredited, the safety of new technological systems acknowledged, and accepted rules of behavior written into the as-yet-unordered domains that have become accessible through knowledge-making (Jasanoff 2004: 39–40).

Perhaps the most well-known example of institutionalised selective connectivity in China is the Great Firewall – a term that refers to everything from restrictions on access to foreign websites (Zhang C. 2020), to comprehensive online censorship (Abbott 2019), to the set of regulations on data localisation to manage cross-border data flows (Liu 2020). The term "Great Firewall" first appeared in a *Wired* article in 1997 (Barme / Ye 1997) but is used likewise in Chinese official newspapers (for example, Global Times 2011). It is a reference to the Great Wall of China, which, according to Selina Ho (2020: 8), represents both the material power of the state to draw together resources from the whole of society, and the symbolic and imagined contrast between the "civilised Chinese" versus the "barbaric others". The Great Firewall is also indicative of the previously mentioned complexity and heterogeneity of actors surrounding cyberspace governance in general (Nye 2014). Just as in the case of the Chinese evolving data governance, various private and public actors are involved in the Great Firewall's functioning, from strategy and policy-setting by the central government to various ministries to private firms (Zhao / Feng 2021, King et al. 2013).

Domestically, the Cybersecurity Law, which officially went into effect on 1 June 2017, defines norms and principles for cybersecurity legislation in China (Creemers 2020). It emphasises the importance of protecting critical information infrastructure that could cause serious damage to national security, the national economy and public interest. China Standards 2035 is another illustration of national policymaking that reflects efforts to reduce technological dependencies and enhance international influence. The document outlines domestic industrial standards and aims to promote the construction of standards systems in key areas, such as blockchain, the Internet of Things, new cloud computing, big data, 5G, new artificial intelligence, new smart cities and geographic information technologies (SAC 2020). China Standards 2035 also proclaims a new emphasis on Chinese industry to shape international standards (The State Council of the People's Republic of China 2021).

These efforts are underpinned by China's "cyber sovereignty" approach to cyberspace governance.[5] In March 2017, China released an international strategy

5 At the 2015 World Internet Conference in Wuzhen, Xi Jinping defined cyber sovereignty as "the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing" (Xi 2015).

on cyber issues – the "International Strategy of Cooperation on Cyberspace" (ISCC). According to the strategy, the goal of China's participation in international cyberspace cooperation is both to safeguard the country's sovereignty and security in cyberspace and to improve global connectivity (The Ministry of Foreign Affairs and the Cyberspace Administration of China 2017).

Cyber sovereignty – a key term in the document – refers to viewing cyberspace as an extension of states' physical territory. It implies a larger role for states in protecting digital infrastructure, processes and internet governance. The "Three-Perspective Theory of Cyber Sovereignty" advanced by Hao Yeli, a retired major general of the People's Liberation Army, provides a layered approach to explain the Chinese vision of cyber sovereignty. Hao (2017) distinguishes between the physical level of cyberspace, in which global connectivity and standardisation are to be pursued; the application level, in which local conditions should determine the balance between cyber sovereignty and freedom; and the "unchallengeable" core level, consisting of regime, law, political security and ideology.

China's interpretation of cyber sovereignty results in a multilateral approach towards internet governance, in which states are more influential than other stakeholders, such as firms and international organisations. Western observers tend to see China's governance approach mostly in opposition to the values of a free and open internet and to the established multi-stakeholder approach of participatory governance (Gady 2016). Over the past years, concerns have broadened that, together with the export of Chinese digital technologies, also the notion of cyber sovereignty is spreading into global governance (Segal 2020). Cyber sovereignty is also increasing the trend towards fragmentation into incompatible national networks (Mueller 2017).

Finally, technical standardisation, as outlined in China Standards 2035, is being directly brought together with foreign policy (Rühlig 2020). For instance, the "Action Plan on Belt and Road Standard connectivity (2018–2020)", issued by the National Development and Reform Commission of China (2018), aims to promote a wider adoption of China's technical standards and supports greater connectivity. China increasingly engages multilateral institutions, such as the ITU, to help establish new standards in the field of telecommunications technology (Cheney 2019). Thanks to massive financial investments and political support from the government, combined with a huge domestic market, Chinese technical companies are strengthening their influence as international global standard-setters. For example, the Chinese telecommunication provider Huawei has played a critical role in setting global technology standards for 5G. The introduction of New IP servers is another important attempt on the part of Huawei to internationalise Chinese government-backed technological standards. According to some observers, the approach "greater involvement by Chinese

companies in multilateral technology standards-setting efforts could materially alter the course of global norms in ways the US and other democracies would not support" (Triolo / Greene 2020).

Performing connectivity

Complementing the institutionally prescribed vision, the STI of selective connectivity is represented by several public performative practices. Public performance here refers to theatrical practices of public communication, deploying visual, verbal and gestural symbols of all kinds.[6] An important part of the performativity of political practice is the (re)framing of new and established vocabularies. Domestically, at the Central Economic Work Conference in December 2018, the State Council introduced the term "New Infrastructures",[7] which refers to technologies such as 5G networks and data centres. New infrastructure is different from traditional infrastructure such as railways, roads and bridges, and mainly refers to key digital facilities in the era of the digital economy (People's Daily Online 2020). It includes three aspects: information infrastructure, innovative infrastructure and integrated infrastructure. In the vision of the Chinese government, new infrastructure construction contributes to greater connectivity and sustainable development through digital industries (Wang 2020).

Internationally, the BRI has made the term connectivity more prominent. Proposed in 2013, the BRI officially has five goals: policy coordination, facilities connectivity, unimpeded trade, financial integration and people-to-people bonds, also summarised as five modes of connectivity (五通, Wu Tong). The BRI's focus on connectivity has a very broad scope including economic, strategic and cultural connectivity (OECD 2018: 10). Connectivity is regarded as "the foundation of development through cooperation". China's president Xi Jinping referred to connectivity in the dimensions of land, maritime, air and cyberspace. He pledged to "promote connectivity of policies, rules and standards so as to provide institutional safeguards for enhancing connectivity" (Xi 2017).

Since announcing the Digital Silk Road (DSR) in 2015, the Chinese government has organised a series of events for and together with European policymakers to enhance global digital connectivity in developing economies. For example, in 2017, China organised a forum on digital connectivity in Qingdao

6 Performativity is an important category for analysing Chinese politics (Ding 2020, Stern et al. 2022). Iza Ding, leaning on a definition by Judith Butler, defines performative governance as "the state's theatrical deployment of visual, verbal, and gestural symbols to foster an impression of good governance before an audience of citizens" (Ding 2020: 5–6).

7 "Xinxing Jijian"(新型基建) or "Xin Jijian" (新基建) for short. New infrastructure includes seven key areas: 5G networks, industrial internet, inter-city transportation and rail system, data centres, artificial intelligence, ultra-high voltage power transmission and new-energy vehicle charging stations.

through the platform of the Asia-Europe Meeting (ASEM). In another 2017 meeting in Brussels, Chinese diplomats joined an ASEM working group to discuss and define connectivity as an ambition for both digital and non-digital spheres of cooperation (Gaens 2019: 9). Gong and Li (2019) argue that China's confidence in promoting the DSR and connectivity abroad draws from domestic lessons on the benefits of building digital infrastructure for rural development. That the imaginary of connectivity is gaining transformative force is evidenced by the DSR initiative to sign up corporations and countries one after another (Eder et al. 2019, Fung et al. 2018).

Another noteworthy example is the "Global Initiative on Data Security" that China announced in September 2020, aiming to establish global standards on data security. This again indicates that, for China, cyber sovereignty is a prerequisite for digital connectivity. As Chinese diplomats advocate for cyber sovereignty, they urge governments to respect other countries' sovereignty in how they handle data collection and protection (Wong 2020). In contrast to this obvious state-centrism, corporate performative elements of China's cyberspace imaginaries focus on the enhancement of commercial connections. Alibaba's record initial public offering on the New York Stock Exchange in 2014 and its opening of e-commerce hubs in Malaysia and Ethiopia were celebrated with great fanfare. Similarly, China's "Single's Day" – an equivalent to the Black Friday shopping event – was internationally promoted on the digital marketplace Lazada and popularised in Southeast Asia (Keane / Yu 2019).

These public performances, however, have sometimes led to unintended effects and responses: sceptical perceptions of China as a cyber power are on the rise. Some assert that the state-led BRI enables China to extend the international influence of its values and norms (Cheney 2019: 11). For instance, American policymakers believe that China is exporting its "techno-authoritarian" model to countries along the BRI (Triolo et al. 2020: 2).

Case Studies: New IP and smart city

To explore the imaginary of selective connectivity further, we focus on two case studies and ask how Chinese actors in these cases institutionalise and perform their visions of infrastructuring cyberspace. The first case examines New IP, an initiative by Huawei and a number of other Chinese organisations to open up research into a new addressing system in cyberspace, put forward at ITU-T in September 2019.[8] Technical standardisation at ITU and other organisations has in recent years grown as a topic of geopolitical interest (Bishop

8 ITU-T, one of three sectors of the International Telecommunication Union, deals with the standardisation of ICT, alongside international organisations such as ICANN and IETF.

2015, Rühlig 2020, Seaman 2020). In the field of cyberspace governance, standardisation is just one in a row of topics that have recently been characterised by disputes between traditionally strong actors from Western countries and powerful newcomers, such as China, but also India and others. The conflicts relate to a variety of issues, such as domain names, distribution of responsibilities, decision-making processes and others (Mueller 2010, Zeng et al. 2017).

The second case is about the Smart City Duisburg, a municipal project in Duisburg, Germany, started in 2017, to digitise the administration and provide a variety of services for its citizens and businesses. Huawei was centrally involved in the planning and testing stages of the project, but eventually saw its cooperation halted due to a combination of persistent negative media coverage and competing local interests. In contrast to international standardisation, projects of urban digital transformation can be seen as local instances of the infrastructuring of cyberspace.[9] Smart cities, in particular, have raised interest in the literature on cyberspace governance due to their contribution to a variety of governance challenges (DeNardis / Raymond 2017). A growing number of scholars are engaging with the role of urban data in the production of global knowledge (Robin / Acuto 2018, Sadowski 2020).

The cases of New IP and the Smart City Duisburg illuminate the implementation of selective connectivity on both global and local scales. In the following, we analyse public communication such as press releases, supported by secondary literature and media articles, to draw a picture of the complexities of China's STI. The coverage of both cases by international media has to some extent pushed the involved actors to position themselves publicly vis-à-vis important technical and political questions.

The New IP proposal

During a September 2019 ITU-T meeting, Huawei, along with the state-owned telecommunications companies China Mobile and China Unicom, and the Chinese Ministry of Industry and Information Technology (MIIT), put forward a proposal for New IP. In the proposal, the firms outlined many challenges the current internet was facing. They proposed to brief ITU-T experts on already conducted research, to initiate strategic planning and to set up new questions for related study groups at the ITU-T. The engineers argued that the current internet design was insufficient for new applications, was already in the process of fragmenting into mutually incompatible technical systems and needed enhanced security and trust (Huawei et al. 2019). To address these challenges, New IP was supposed to enhance current IP by introducing addresses of different length, semantics

9 A smart city can be defined as a city "connecting the physical infrastructure, the information-technology infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city" (Mohanty et al. 2016: 1).

to identify objects and user-definable IP headers (Chen et al. 2020).[10] Huawei estimated that the investments and business value of New IP would run into trillions of US dollars (Sheng 2019: 21). In the weeks and months that followed, Huawei presented New IP at an ITU workshop (in October 2019), at a side meeting to the Internet Engineering Task Force (IETF)[11] (in November 2019) and at various other meetings at ITU and IETF.[12]

Initial reactions were sceptical about New IP's technical capabilities. For example, the Internet Corporation for Assigned Names and Numbers (ICANN), which is responsible for coordinating the maintenance and procedures of several databases, questioned the interoperability of New IP with the earlier protocols IPv4 and IPv6. Moreover, experience with IPv6 had shown that complete replacement of old protocols would probably take decades (Durand 2020: 24–25). Similarly, IETF (2020) argued that New IP could not provide a solution to the problem of interoperability, and that the replacement of existing IP would "most assuredly create network islands, damage interconnection, and jeopardise interoperability".

The topic of New IP reached a broader public through two articles in the *Financial Times* in March 2020 (Gross / Murgia 2020, Murgia / Gross 2020). In the articles, the authors described the New IP proposal in the context of broader debates about the future of cyberspace and the geopoliticisation of internet governance. They argued:

> Whereas today's internet is owned by everyone and no one, [New IP] could put power back in the hands of nation states, instead of individuals (Murgia / Gross 2020).

This line of argument was picked up by other commentators, who pointed out how certain envisaged characteristics of New IP would be especially favourable to the state-centric internet governance model. According to ICANN, the deployment of New IP would facilitate digital surveillance:

> [New IP involves] a strong regulatory binding between an IP address and a user [that] would allow any intermediary element (router, switch, and so on) to have full access to exactly which user is doing what (Durand 2020: 3).

The technical possibilities of New IP have political implications that could, according to some views, ultimately "splinter the global internet's shared and ubiquitous architecture" (Hoffmann et al. 2020: 239). A substantially different software infrastructure would thus deepen the rift between two opposing camps in a long-standing debate about internet governance reform: on the one hand, those states pursuing an open internet, and, on the other hand, those states perceiving benefits from more centralised governmental control (Deep 2020).

10 Routing means to designate parts of an IP address for certain purposes (Farrel / King 2022).

11 IETF is an important Internet standards organisation, which is responsible to develop the technical standards that make up the Internet protocol suite.

12 See ITU-T 2020; Network 2030, Description of Demonstrations for Network 2030 on Sixth ITU Workshop on Network 2030 and Demo Day, 13 January 2020.

Another point of criticism was related to the fact that the Chinese companies had presented the proposal to ITU-T rather than (only) to IETF. IETF (2020) argued that the creation of a top-down design of New IP "would fail to match the diverse needs of the continuously evolving application ecosystem". The European Telecommunications Network Operators' Association (ETNO) explained that a shift of responsibility from the IETF to the ITU-T would represent a duplication of standardisation work (ETNO 2020). RIPE Network Coordination Centre (NCC), one of five Regional Internet Registries (RIR), agreed that the New IP proposal would create significant overlap with the ongoing work of the IETF (ITU 2020). This point of criticism reflected the sense of mutual competition between ITU and IETF, which had both developed capacities to regulate certain aspects of cyberspace.

These institutional rivalries over responsibilities need to be situated within more general discourses about China's dissatisfaction with the global internet governance regime (Shen Y. 2016). For years, some authors have argued that China would prefer to shift more responsibility for internet governance to ITU, where states are more dominant than in ICANN or the RIRs (Mueller 2011). As a consequence, so the argument, China wanted to reshape internet governance so that it is more aligned with its vision and norms (Bozhkov 2020). Moreover, others suggested that, by proactively pursuing international standardisation, China aims to create and protect potential markets for its globally active large tech corporations (Hoffmann et al. 2020: 246). Presenting New IP at ITU-T thus reflected China's approach to shift internet governance into a direction more in line with its domestic agenda and approach (Sharma 2020).

After a barrage of critical commentary on New IP, Huawei lamented the politicisation of New IP: "New IP is just a purely technical topic. Don't politicise New IP from the beginning," Huawei's rotating chairman Xu Zhijun stated in an interview (Zhang P. 2020). Others tried to maintain a more measured position. For example, Milton Mueller, a renowned scholar in the field of internet governance, argued that the Internet community should resist the tacit politicisation of technical standards (Mueller 2020). Eventually, at ITU-T study group meetings during December 2020, the decision was taken to stop discussing New IP for a while.[13]

Smart City Duisburg

Huawei's involvement with Duisburg reaches back to 2017, when Duisburg was in the process of developing a master plan for the city's digital transformation and was looking for hardware and technological expertise (Ahlemann / Murrack 2018). In October 2017, Huawei and Duisburg signed a Memorandum

13 Yet, according to some observers, elements of the proposal have since appeared in various places (Bertuzzi 2022, Internet Society 2022: 3).

of Understanding (MoU) in Shenzhen (Huawei 2017). The MoU was meant to summarise the current vision and agreements and facilitate further talks on the development of "innovative ICT concepts for intelligent and safe cities" (Stadt Duisburg / Huawei 2017: 2). Huawei stated that it wanted to work on projects together with the municipal firms DVV and DU-IT, stimulate the development of 5G, and share its technical know-how with the city administration and the University of Duisburg-Essen.[14] In January 2018, during another delegation visit by Duisburg to Huawei in Shenzhen, the partners formally announced the smart city cooperation to the public (Huawei 2018a, Stadt Duisburg 2018).

Huawei's management made the Smart City Duisburg a major reference point in its promotion of smart city technologies, and continually expanded the cooperation with Duisburg. In June 2018, Huawei invited Duisburg's head of digitalisation Martin Murrack and the CEO of DU-IT, Stefan Soldat, to deliver speeches at the CEBIT fair in Hanover (Bordel 2018, Smart City Duisburg 2018). In July 2018, Huawei, along with several other organisations from Duisburg, signed a letter of intent to enter into cooperation for the smart city (Stadt Duisburg 2019a: 14). In September 2018, Duisburg's mayor led another delegation to visit Huawei's headquarters in Shenzhen (Huawei 2018b). And in October 2018, at a conference organised by Huawei, Huawei presented Duisburg as a critical example of its international smart city cooperation (Huawei 2018c).

A key piece of Huawei's vision of a fully interconnected smart city was the Rhine Cloud, a cloud infrastructure jointly provided by Huawei and DU-IT (Huawei 2018d). All collected data would be stored in the Rhine Cloud to service citizens and business users. The Rhine Cloud was to serve as the foundation of the smart city nervous system (Huawei 2018e: 13), perhaps even the "brain" and "command centre", modelled after a Huawei project in Longgang district of Shenzhen (Huawei 2018f, Huawei 2018g). Using the Rhine Cloud, Duisburg could "break down data silos", complete the first stage of smart city development, and reach towards the "Smart Duisburg 2.0 vision" (Huawei 2018h, 2018g). Smart city 3.0 would then use the Internet of Things to "truly integrate technology and urban governance" (Huawei 2018e: 5). In the fourth stage, cities would use artificial intelligence to continually analyse urban data for governance purposes (Huawei 2018g). In July 2018, Duisburg explained that the Rhine Cloud was already in operation (Ahlemann / Murrack 2018: 4).

Soon after its announcement, the cooperation between Huawei and Duisburg was taken up by a wide range of national and international actors, including from media, academia and civil society. Many reports were critical about the cooperation, arguing that it was a security risk to involve a foreign, and especially a Chinese, company in the provision of data sensitive infrastructure. Moreover,

14 DU-IT is a subsidiary of DVV, which belongs to Duisburg municipality (Stadt Duisburg 2021: 4).

Huawei's smart city vision, as realised in Longgang, Shenzhen, demonstrated a level of interconnected surveillance that was incompatible with German laws and regulations (Sassenrath 2019, WAZ 2019). A research report, prepared for the US-China Economic and Security Review Commission, described the Chinese smart city projects, including the one in Duisburg, as a means for Chinese firms to expand abroad, source foreign technology and expertise, develop partnerships, promote Chinese technology standards and improve their international reputation (Atha et al. 2020).

After September 2019, when Duisburg's city council approved the master plan for digital transformation (Stabsstelle Digitalisierung 2019, Stadt Duisburg 2019b), public communication from both Duisburg and Huawei about the cooperation ceased. Since the beginning of 2021, media articles have begun to mention that the cooperation with Huawei has been put on hold due to security considerations (Prantner 2021). Despite that pause, Duisburg continues to elaborate on its China strategy, as the city has developed a new understanding of its global connections due to its interactions with Huawei.[15]

Discussion: The politics of selective connectivity

The exploration of China's infrastructuring of cyberspace raises a number of questions. First, there is a tension between the performative practices of Chinese actors that celebrate boundless connectivity versus the efforts to institutionalise national security and digital autonomy. In the smart city case, Huawei was very proactive in communicating with its partners and the public. China was presented as an example of connected modernity symbolised by Shenzhen as the smart city par excellence. Issues such as data privacy and digital sovereignty, which could interfere with the global leadership of Chinese tech firms (Holch 2020), were played down. In the case of New IP, Huawei and the other initiators did not publicise much of their activity. The performative side of connectivity was superseded by efforts to institutionalise research into a technology. How New IP was introduced, in addition, intended to give a greater role to the ITU, where states have more say, in contrast to IETF and other fora, where states are less influential. Overall, the practices of selective connectivity, while contributing to the development of the digital economy, also tend to increase asymmetries and vulnerabilities, by creating new obligatory passage points and thereby enabling the potential weaponization of telecommunication and data infrastructures.

Second, the importance of non-Chinese agency is underappreciated, as the ultimate failure of infrastructuring in these two examples suggests. The discus-

15 Interviews by the authors with involved city representatives conducted in 2021 and 2022.

sion of the weaponisation of interdependence is arguably a case in point (Farrell / Newman 2019). China and Chinese firms insert themselves into the central nodes of global cyber networks, so the argument goes, to occupy choke points that enable them to potentially monitor internet traffic (Cavanna 2021). New IP, due to its centralising tendencies, would likely be more vulnerable to weaponisation. In the smart city as imagined by Huawei, the actor controlling the city's central server architecture and envisioned artificial intelligence would gain the opportunity to misuse its critical position at the centre of data flows. However, as is evident from the cases, contestations over knowledge claims and diverging views on data security led to a pause or even a complete halt of infrastructure projects.[16] Chinese actors, in other words, cannot simply export political norms through technology, as is often claimed (Cheney 2019). In brief, attempts at infrastructuring cyberspace call forth responses from other actors while the realisation of China's own vision and practices has to rely on consensual negotiations.

Third, China's imaginary of selective connectivity reinforces a growing mistrust that undermines the internationalisation of Chinese firms, especially in Western countries. It contributes to an unfavourable global economic environment in which geopolitics can easily trump commercial logic. Domestically, Chinese firms need to comply with regulations on national and public security. Those same practices are frowned upon by international users (Ruan 2019). China's growing standardisation power similarly invokes anxieties and critical analysis of the central role the Chinese state plays in related activities (Rühlig 2022, Rühlig / ten Brink 2021). Moreover, the increasing popularity of notions such as cyber sovereignty and digital sovereignty – which Chinese officials have been actively promoting – lends legitimacy to the restrictions by the United States and its allies against Chinese firms and products. US commenters supported the Trump administration's ban of the Chinese apps TikTok and WeChat as a tit for tat because many American Internet companies have been blocked in China for years (Wu 2020).

Fourth, the Chinese STI has lost its uniqueness. The imaginary of selective connectivity is no longer only characteristic of China's approach to cyberspace. It has become normalised internationally as a vision related to the growig prominence of the notion of „digital sovereignty" (see Monsees / Lambach 2022). For instance, a comparison of China's and the EU's respective "sovereignty" approaches to the regulation of cyberspace indicates a partially shared understanding of the regulatory challenges that digital platform monopolies pose to market economies (Wang / Gray 2022). It needs to be noted that this convergence is not due to the success of Chinese diplomatic efforts and the adoption of Chinese norms. Instead, a growing number of countries embrace cyber sovereignty because of "threats to

16 The New IP proposal made factual claims about the desired data transmission speed. The need and (im) possibility for achieving global sub-millisecond latencies due to the limitations of the speed of light were questioned by other expert bodies (Internet Society 2022: 6).

privacy, and concentration of economic and political power by big technology firms" (Segal 2020). Furthermore, on a structural level, this convergence stems from the confluence of several global trends such as platform regulation, data nationalism and the discourse of systemic confrontation (see Huang / Tsai 2022, Paris 2020) – all of which tend to render selective connectivity the new normal.

Conclusion

This paper applied the framework of sociotechnical imaginaries to explore China's vision and practices of infrastructuring cyberspace. China's imaginary of selective connectivity is characterised by a tension between seeking more connectivity – realised by strong private firms in the Chinese ICT sector – and, at the same time, institutionalising measures to control the flow of data and information to ensure national security and regime stability. The notion of cyber sovereignty, which has already found its way into international fora and settings, exemplifies the constitutive power of China's imaginary of selective connectivity. Yet, the two case studies on New IP and the Smart City Duisburg also demonstrate the drawbacks of this imaginary. In the case of New IP, Huawei communicated its proposal to work on a new, potentially more centralised internet architecture as a way to facilitate more connectivity and high-tech applications. The underlying technology raised concerns. It would, as some argued, not only create problems of interoperability in the short term; it also would hand more power to national agencies. In the case of the Smart City Duisburg, Huawei promoted a vision of ubiquitous connectivity, including a levelling up of cities. Its perceived model of a smart city in Shenzhen, powered by a central artificial intelligence, led to serious concerns as it exhibited characteristics potentially prone to centralised control.

Four conclusions can be drawn from this study concerning selective connectivity to advance further research into the splintering of the internet: First, the realisation of China's imaginary abroad strongly depends on Chinese private firms, which are not always in line with the state-centric vision of Chinese policymakers. Second, the manifestation of selective connectivity may cause tensions between a heterogenous set of Chinese actors promoting connectivity and the Chinese government's simultaneous efforts to institutionalise state-centric regulation. Third, how other actors respond to and contest China's vision and practices plays a crucial role in shaping the outcome of cyber infrastructure projects. Fourth, China's imaginary of selective connectivity may eventually make the internationalisation of Chinese companies difficult, for example, by providing legitimacy to other countries' bans of Chinese companies and products.

Finally, some limitations of this study need to be addressed. The underlying theory of sociotechnical imaginaries tends to deemphasise differences and heterogeneity. On the one hand, we can observe that selective connectivity as a vision is sufficiently flexible and attractive to assemble various types of actors. To begin with, the realisation of digital infrastructure projects depends to a large extent on private technology companies (Meinhardt 2020). Due to good relationships that large firms in China need to maintain with officials, proposals like New IP and Huawei's global smart city initiatives could be seen as closely corresponding with the Chinese government's policy visions.[17] On the other hand, the STI held by Chinese policymakers does not always completely overlap with that of Chinese digital tech giants. On the contrary, the domestic struggle over regulation reveals far-reaching conflicts of interest between tech firms and the country. This is obvious from the recent high-profile cases of industry regulation that led to a USD 1 billion fine for ride-hailing giant DiDi and a record USD 2.75 billion antitrust fine against Alibaba (Zhu et al. 2022) – public demonstrations that it is the state-led vision of connectivity rather than corporate-led visions that prevails. Elsewhere, Alibaba promoted a "limited government intervention" model, which was in contradiction with the Chinese state-centric internet governance model (Vila Seoane 2020). In sum, the STI of selective connectivity is not sufficient to capture the full range of complexities of China's infrastructural politics.

17 Because of the complex technical nature of digital infrastructure, it seems reasonable to assume that political guidance must be on a rather high, abstract level, and is unlikely to extend down into the technical details of individual products and projects. In any case, in the explored cases, practices by Huawei do not run contrary to and reproduce to some extent the government-promoted STI of selective connectivity.

References

Abbott, Jason P. (2019): Of Grass Mud Horses and Rice Bunnies: Chinese Internet Users Challenge Beijing's Censorship and Internet Controls. *Asian Politics and Policy* 11(1), pp. 162–168.

Ahlemann, Frederik / Martin Murrack (2018): Vorstellung Kernpunkte Masterplan Digitales Duisburg. Presented at the Auftaktveranstaltung Smart City Duisburg. https://www.duisburg.de/allgemein/fachbereiche/digitalisierung.php.media/70447/Smart_City_Auftaktveranstaltung_-_Masterplan_Digitales_Duisburg_v07_FAh.pdf (accessed 25 July 2022).

Alsen, Daniel / Patel, Mark / Shangkuan, Jason (2017): The Future of Connectivity: Enabling the Internet of Things. McKinsey & Company, 29 November, https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/the-future-of-connectivity-enabling-the-internet-of-things (accessed 24 July 2022).

ASEAN (2011): *Master Plan on ASEAN Connectivity*. 1st Reprint. Jakarta: ASEAN Secretariat, Public Outreach and Civil Society Division.

Atha, Katherine / Callahan, Jason / Chen, John / Drun, Jessica / Francis, Ed / Green, Kieran / Lafferty, Brian / McReynolds, Joe / Mulvenon, James / Rosen, Benjamin / Walz, Emily (2020): China's Smart Cities Development. Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission. SOS International LLC, https://www.uscc.gov/research/chinas-smart-cities-development (accessed 24 July 2022).

Bach, Jonathan (2016): China's Infrastructural Fix. *Limn* 7, https://limn.it/articles/chinas-infrastructural-fix/ (accessed 24 July 2022).

Barker, Joshua (2015): Guerilla Engineers: The Internet and the Politics of Freedom in Indonesia. In: Sheila Jasanoff / Sang-Hyun Kim (eds): *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power*. Chicago / London: University of Chicago Press, pp. 199–218.

Barme, Geremie R. / Ye, Sang (1997): The Great Firewall of China. *Wired*, 6 January, https://www.wired.com/1997/06/china-3/ (accessed 24 July 2022).

Bertuzzi, Luca (2022): China Rebrands Proposal on Internet Governance, Targeting Developing Countries. Euractiv, 6 June, https://www.euractiv.com/section/digital/news/china-rebrands-proposal-on-internet-governance-targeting-developing-countries/ (accessed 6 July 2022).

Bishop, Andrew D. (2015): Standard Power: The New Geopolitical Battle. *The National Interest*, 7 October, https://nationalinterest.org/feature/standard-power-the-new-geopolitical-battle-14017 (accessed 24 July 2022).

Bordel, Stefan (2018): Smart City auf der CEBIT: Huawei digitalisiert Duisburg. *Com - Das Computer-Magazin*, 12 June, https://www.com-magazin.de/news/digitalisierung/huawei-digitalisiert-duisburg-1545200.html (accessed 28 June 2021).

Bozhkov, Nikolay (2020): *China's Cyber Diplomacy: A Primer*. EU Cyber Direct.

Cai, Cuihong / Dai, Liting (2021): Evolution of Internet Governance in China: Actors and Paradigms. *China Quarterly of International Strategic Studies* 7(1), pp. 79–109.

Castells, Manuel (2010): *The Rise of the Network Society*. 2nd edition. Cambridge: Blackwell Publishing.

Cavanna, Thomas P. (2021): Coercion Unbound? China's Belt and Road Initiative. In: Daniel W. Drezner / Henry Farrell / Abraham L. Newman (eds): *The Uses and Abuses of Weaponized Interdependence*. Washington: Brookings Institution Press.

Cheney, Clayton (2019): China's Digital Silk Road: Strategic Technological Competition and Exporting Political Illiberalism. Council on Foreign Relations, 26 September, https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political (accessed 24 July 2022)."

Chen, Zhe / Wang, Chuang / Li, Guanwen / Lou, Zhe / Jiang, Sheng / Galis, Alex (2020): New IP Framework and Protocol for Future Applications. IEEE/IFIP Network Operations and Management Symposium, pp. 1–5. https://doi.org/ 10.1109/NOMS47738.2020.9110352

Choy, Pinky D. W. / Cullen, Richard (1999): The Internet in China. *Columbia Journal of Asian Law* 13(1), pp. 99–134.

Cox, Michael (2017): The Rise of Populism and the Crisis of Globalisation: Brexit, Trump and Beyond. *Irish Studies in International Affairs* 28, pp. 9–17.

Creemers, Rogier (2020): China's Conception of Cyber Sovereignty: Rhetoric and Realization. In: Dennis Broeders / Bibi van den Berg (eds): *Governing Cyberspace: Behavior, Power, and Diplomacy*. Lanham: Rowman & Littlefield, pp. 107–144.

Deep, Aroon (2020): What Huawei and China's New IP Proposal Is All About. MediaNama, 7 October, https://www.medianama.com/2020/10/223-new-ip-huawei-china/ (accessed 24 July 2022).

Deibert, Ronald / Palfrey, John / Rohozinski, Rafal / Zittrain, Jonathan (2010): *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge: The MIT Press.

DeNardis, Laura / Raymond, Mark (2017): The Internet of Things as a Global Policy Frontier. *U.C. Davis Law Review* 51(2), pp. 475–498.

Ding, Iza (2020): Performative Governance. *World Politics* 72(4), pp. 525–556.

Diamond, Larry (2019): The Road to Digital Unfreedom: The Threat of Postmodern Totalitarianism. *Journal of Democracy* 30(1), pp. 20–24.

Drake, William J. / Cerf, Vinton G. / Kleinwächter, Wolfgang (2016): Internet Fragmentation: An Overview. World Economic Forum, January, https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf (accessed 24 July 2022)

Drezner, Daniel W. (2004): The Global Governance of the Internet: Bringing the State Back. *Political Science Quarterly* 119(3), pp. 477–498.

Drezner, Daniel W. / Farrell, Henry / Newman, Abraham L. (eds) (2021): *The Uses and Abuses of Weaponized Interdependence*. Washington: Brookings Institution Press.

Durand, Alain (2020): New IP. ICANN Office of the Chief Technology Officer, 27 October, https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf (accessed 24 July 2022).

Eder, Thomas S. / Arcesati, Rebecca / Mardell, Jacob (2019): Networking the "Belt and Road." The Future Is Digital. MERICS, 28 August, https://merics.org/en/analysis/networking-belt-and-road-future-digital (accessed 24 July 2022).

Edwards, Paul N. (2003): Infrastructure and Modernity: Force, Time, and Social Organization in the History of Sociotechnical Systems. In: Thomas J. Misa / Philip Brey / Andrew Feenberg (eds): *Modernity and Technology*. Cambridge, Mass. / London: The MIT Press, pp. 185–225.

ETNO – European Telecommunications Network Operators' Association (2020): ETNO Position Paper on the New IP Proposal. ETNO, 5 November, https://etno.eu/library/417-new-ip.html (accessed 24 July 2022).

People's Daily Online (2020): "New Infrastructure" in Digital Era to Boost Chinese Economy. *People's Daily Online*, 16 March, http://en.people.cn/n3/2020/0316/c90000-9668794.html (accessed 24 July 2022).

Farrel, Adrian / King, Daniel (2022): An Introduction to Semantic Routing. IETF, 25 April 2022, https://www.ietf.org/id/draft-farrel-irtf-introduction-to-semantic-routing-04.html (accessed 24 July 2022).

Farrell, Henry / Newman, Abraham L. (2019): Weaponized Interdependence: How Global Economic Networks Shape State Coercion. *International Security* 44(1), pp. 42–79.

Felt, Ulrike (2015): Sociotechnical Imaginaries of "the Internet", Digital Health Information and the Making of the Citizen-patients. In: Stephen Hilgartner / Clark A. Miller / Rob Hagendijk (eds): *Science and Democracy. Making Knowledge and Making Power in the Biosciences and beyond*. New York: Routledge, Taylor & Francis Group, pp.176–197.

Fontaine, Richard (2020): Globalization Will Look Very Different After the Coronavirus Pandemic. *Foreign Policy*, 17 April, https://foreignpolicy.com/2020/04/17/globalization-trade-war-after-coronavirus-pandemic/ (accessed 24 July 2022).

Fung, K.C. / Aminian, Nathalie / Fu, Xiaoqing (Maggie) / Tung, Chris Y. (2018): Digital Silk Road, Silicon Valley and Connectivity. *Journal of Chinese Economic and Business Studies* 16(3), pp. 313–336.

Gady, Franz-Stefan (2016): The Wuzhen Summit and the Battle over Internet Governance. *The Diplomat*, 14 January, https://thediplomat.com/2016/01/the-wuzhen-summit-and-the-battle-over-internet-governance/ (accessed 24 July 2022).

Gaens, Bart (2019): The EU-Asia Connectivity Strategy and Its Impact on Asia-Europe Relations. Konrad-Adenauer-Stiftung, https://www.kas.de/documents/288143/6741384/panorama_trade_BartGaensTheEU-AsiaConnectivityStrategyandItsImpactonAsia-EuropeRelations.pdf (accessed 24 July 2022).

Giddens, Anthony (1990): *The Consequences of Modernity*. Cambridge: Polity Press.

Global Times (2011): Great Firewall Father Speaks Out. China.org, 18 February, http://www.china.org.cn/china/2011-02/18/content_21951602.htm (accessed 24 July 2022).

Global Times (2022): China Has 1.032 Billion Internet Users, 73.0% Penetration Rate. *Global Times*, 25 February, https://www.globaltimes.cn/page/202202/1253226.shtml (accessed 11 July 2022).

Godehardt, Nadine / Kohlenberg, Paul J. (2020): China's Global Connectivity Politics: A Meta-geography in the Making. In: Paul J. Kohlenberg / Nadine Godehardt (eds): *The Multidimensionality of Regions in World Politics*. Abingdon / New York: Routledge, pp. 191–215.

Gong, Sen / Li, Bingqin (2019): The Digital Silk Road and the Sustainable Development Goals. *IDS Bulletin* 50(4), pp. 23–46, Brighton: IDS.

Gore, Al (1991): Infrastructure for the Global Village. *Scientific American* 265(3), pp. 150–153.

Gross, Anna / Murgia, Madhumita (2020): China and Huawei Propose Reinvention of the Internet. *Financial Times*, 27 March, https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2 (accessed 24 July 2022).

Hao, Yeli (2017): A Three-Perspective Theory of Cyber Sovereignty. *PRISM* 7(2), pp. 109–115.

Herrera, Geoffrey L. (2002): The Politics of Bandwidth: International Political Implications of a Global Digital Information Network. *Review of International Studies* 28(1), pp. 93–122.

Hill, Jonah Force (2012): Internet Fragmentation. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Hill, Jonah Force (2014). The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders. The Hague Institute for Global Justice, Conference on the Future of Cyber Governance, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2430275 (accessed 24 July 2022).

Ho, Selina (2020): Infrastructure and Chinese Power. *International Affairs* 96(6), pp. 1461–1485.

Hoffmann, Stacie / Lazanski, Dominique / Taylor, Emily (2020): Standardising the Splinternet: How China's Technical Standards Could Fragment the Internet. *Journal of Cyber Policy* 5(2), pp. 239–264.

Holch, Gabor (2020): WeChat, Zoom, TikTok and the Future of Chinese Technology Culture. Asia Power Watch, 25 September, https://asiapowerwatch.com/wechat-zoom-tiktok-and-the-future-of-chinese-technology-culture/ (accessed 24 July 2022).

Hong, Yu (2017): Networking China: The Digital Transformation of the Chinese Economy. Urbana / Chicago / Springfield: University of Illinois Press (Geopolitics of Information).

Huang, Jingyang / Tsai, Kellee S. (2022): Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China. *The China Journal* 88(1), pp. 2–28.

Huang, Ying / Mayer, Maximilian (2022): Digital Currencies, Monetary Sovereignty, and U.S.-China Power Competition. *Policy & Internet* 14(2), pp. 324–347.

Huawei / China Mobile / China Unicom / Ministry of Industry and Information Technology (2019): "New IP, Shaping Future Network": Propose to Initiate the Discussion of Strategy Transformation for ITU-T. Geneva, 23–27 September, International Telecommunication Union TSAG-C83.

Huawei (2018a): Huawei und Duisburg vereinbaren Zusammenarbeit für die Entwicklung Duisburgs zur Smart City. Huawei, 15 January https://e.huawei.com/de/news/de/2018/huawei-und-duisburg-zusammenarbeit-smart-city (accessed 24 July 2022).

Huawei (2018b): Huawei vertieft Kooperation mit Duisburg, um den deutschen Industriestandort in eine neue Smart City zu verwandeln. Huawei, 3 September, https://e.huawei.com/de/news/de/2018/Huawei_vertieft_Kooperation_mit_Duisburg (accessed 24 July 2022).

Huawei (2018c): Mit künstlicher Intelligenz zu besseren Smart Cities. Huawei, 10 October, https://e.huawei.com/de/news/de/2018/activate-intelligence-to-build-better-smart-cities (accessed 24 July 2022).

Huawei (2018d): Huawei and DU-IT Help Duisburg Become a Smart City. Huawei, 11 June, https://www.huawei.com/en/news/2018/6/Huawei-DU-IT-Duisburg-SmartCity (accessed 24 July 2022).

Huawei (2018e): Better Governance, Better Livelihood, and Better Industry: New ICT, Creating a Smart City Nervous System. Huawei, 10 June, https://e.huawei.com/en/material/industry/smartcity/02ad4d5ab60849-2ea24659ec667f04bd (accessed 24 July 2022).

Huawei (2018f): Huawei Deepens Cooperation with Duisburg to Transform Germany's Industrial Heartland into a Smart City. Huawei, 3 September, https://www.huawei.com/en/news/2018/9/huawei-duisburg-germany-smartcity (accessed 24 July 2022).

Huawei (2018g): Huawei Launches Digital Platform for Smart Cities at Smart City Expo World Congress 2018. Huawei, 13 November, https://www.huawei.com/en/news/2018/11/digital-platform-smart-cities-smart-city-expo-world-congress-2018 (accessed 24 July 2022).

Huawei (2018h): Activate Intelligence to Build Better Smart Cities. Huawei, 11 October, https://e.huawei.com/en/news/global/2018/HC2018/201810111600 (accessed 24 July 2022).

IETF (2020): Liaison Statement. Response to "LS on New IP, Shaping Future Network". IETF, 30 March, https://datatracker.ietf.org/liaison/1677/ (accessed 24 July 2022).

Internet Society (2022): Huawei's "New IP" Proposal: Frequently Asked Questions. Internet Society, 22 February, https://www.internetsociety.org/resources/doc/2022/huaweis-new-ip-proposal-faq/ (accessed 07 July 2022).

Isin, Engin F. / Ruppert, Evelyn Sharon (2020): *Being Digital Citizens*. 2nd edition. London / New York: Rowman & Littlefield.

ITU (2020): Response to "New IP, Shaping Future Network" Proposal. TSAG-C0135-Contribution, 10–14 February, Geneva, https://www.ripe.net/participate/internet-governance/multi-stakeholder-engagement/ripe-ncc_tsag_new-ip.pdf (accessed 24 July 2022).

Jasanoff, Sheila (2004): Ordering Knowledge, Ordering Society. In: Sheila Jasanoff (ed.): *States of Knowledge: The Co-production of Science and Social Order.* London / New York: Routledge, pp. 13–45.

Jasanoff, Sheila (2015): Future Imperfect: Science, Technology, and the Imaginations of Modernity. In: Sheila Jasanoff / Sang-Hyun Kim (eds): *Dreamscapes of Modernity. Sociotechnical Imaginaries and the Fabrication of Power.* Chicago / London: University of Chicago Press, pp. 1–33.

Jasanoff, Sheila / Kim, Sang-Hyun (2009): Containing the Atom: Sociotechnical Imaginaries and Nuclear Power in the United States and South Korea. *Minerva* 47(2), pp. 119–146.

Jasanoff, Sheila / Kim, Sang-Hyun (eds) (2015): Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power. Chicago: University of Chicago Press.

Keane, Michael / Yu, Haiqing (2019): A Digital Empire in the Making: China's Outbound Digital Platforms. *International Journal of Communication* 13(0), p. 18.

Keohane, Robert O. / Nye, Joseph S. (2012): *Power and Interdependence*. 4th edition. Boston: Longman.

King, Gary / Pan, Jennifer / Roberts, Margaret E. (2013): How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review* 107(2), pp. 326–343.

Korn, Matthias / Reißmann, Wolfgang / Röhl, Tobias / Sittler, David (eds) (2019): *Infrastructuring Publics*. Wiesbaden: Springer Fachmedien Wiesbaden.

Kuehl, Daniel T. (2009): From Cyberspace to Cyberpower: Defining the Problem. In: Franklin Kramer / Stuart H. Starr / Larry Wentz (eds): *Cyberpower and National Security*. National Defense University Press: Potomac Books, pp. 24–42.

Lengen, Samuel (2022): Digital Imaginaries and the Chinese Nation State. In: Irfan Ahmad / Jie Kang (eds): *The Nation Form in the Global Age: Ethnographic Perspectives*. Cham: Palgrave Macmillan, pp. 203–223.

Leonard, Mark (2016): Connectivity Wars. Why Migration, Finance and Trade Are the Geo-economic Battlegrounds of the Future. European Council on Foreign Relations, https://ecfr.eu/wp-content/uploads/Connectivity_Wars.pdf (accessed 25 July 2022).

List, Friedrich (1885): *The National System of Political Economy*. London: Longmans, Green and Co. https://oll-resources.s3.us-east-2.amazonaws.com/oll3/store/titles/315/0168_Bk.pdf (accessed 25 July 2022).

Liu, Jinhe (2020): China's Data Localization. *Chinese Journal of Communication* 13(1), pp. 84–103.

Lu, Xiaomeng (2020): Is China Changing Its Thinking on Data Localization? *The Diplomat*, 4 June, https://thediplomat.com/2020/06/is-china-changing-its-thinking-on-data-localization/ (accessed 24 July 2022).

Lund, Susan / Manyika, James / Woetzel, Jonathan / Bughin, Jacques / Krishnan, Mekala / Seong, Jeongmin / Muir, Mac (2019): Globalization in Transition: The Future of Trade and Value Chains. McKinsey & Company, https://www.mckinsey.com/featured-insights/innovation-and-growth/globalization-in-transition-the-future-of-trade-and-value-chains (accessed 24 July 2022).

Mahoney, Josef Gregory (2022): China's Rise as an Advanced Technological Society and the Rise of Digital Orientalism. *Journal of Chinese Political Science* (2022). https://doi.org/10.1007/s11366-022-09817-z

Malcomson, Scott (2016): *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web*. London: OR Books.

Monsees, Linda / Lambach, Daniel (2022): Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity. *European Security* 31(3), pp. 377–394.

Munn, Luke (2020): Red Territory: Forging Infrastructural Power. *Territory, Politics, Governance* (October), pp. 1–20. https://doi.org/10.1080/21622671.2020.1805353

Mattelart, Armand (2000): *Networking the World, 1794–2000*. Minneapolis / London: University of Minnesota Press.

Mayer, Maximilian (2020): China's Authoritarian Internet and Digital Orientalism. In: Denise Feldner (ed.): *Redesigning Organizations: Concepts for the Connected Society*. Cham: Springer, pp. 177–192.

Mayer, Maximilian / Acuto, Michele (2015): The Global Governance of Large Technical Systems. *Millennium* 43(2), pp. 660–683.

Mayer, Maximilian / Huotari, Mikko (2015): China: Geopolitik durch Infrastruktur. *Blätter für Deutsche und Internationale Politik* 60(7), pp. 37–40.

Meinhardt, Caroline (2020): China Bets on "New Infrastructure" to Pull the Economy out of Post-Covid Doldrums. Mercator Institute for China Studies, https://merics.org/en/analysis/china-bets-new-infrastructure-pull-economy-out-post-covid-doldrums (accessed 24 July 2022).

Mohanty, Saraju P. / Choppali, Uma / Kougianos, Elias (2016): Everything You Wanted to Know about Smart Cities. *IEEE Consumer Electronics Magazine* 5(3), pp. 60–70, https://ieeexplore.ieee.org/document/7539244 (accessed 24 July 2022).

Mueller, Milton (2010): *Networks and States: The Global Politics of Internet Governance*. Cambridge: The MIT Press.

Mueller, Milton (2011): China and Global Internet Governance. In: Ronald Deibert / John Palfrey / Rafal Rohozinski / Jonathan Zittrain (eds): *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. Cambridge / London: The MIT Press, pp. 177–192.

Mueller, Milton (2017): *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*. Cambridge, Malden: Polity Press.

Mueller, Milton (2020): About that Chinese "Reinvention" of the Internet. Internet Governance Project, 30 March https://www.internetgovernance.org/2020/03/30/about-that-chinese-reinvention-of-the-internet/ (accessed 24 July 2022).

Murgia, Madhumita / Gross, Anna (2020): Inside China's Controversial Mission to Reinvent the Internet. *Financial Times*, 27 March 2020, https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f (accessed 24 July 2022).

Murphy, Flinn / Tong, Qian (2021): In Depth: Pushback against China Tech Giants Grows with Accusation of Algorithmic "Bullying". *Caixin Global*, 14 January, https://www.caixinglobal.com/2021-01-14/in-depth-pushback-against-china-tech-giants-grows-with-accusation-of-algorithmic-bullying-101650876.html (accessed 15 July 2022).

Nikkei (2020): Divided Internet. China and US Switch Places as Data Powerhouse. Vdata, 23 November, https://vdata.nikkei.com/en/newsgraphics/splinternet/ (accessed 24 July 2022).

Nussbaum, Bruce (2010): Peak Globalization. *Harvard Business Review*, 20 December, https://hbr.org/2010/12/peak-globalization (accessed 24 July 2022).

Nye, Joseph S. (2014): The Regime Complex for Managing Global Cyber Activities. Centre for International Governance Innovation and the Royal Institute for International Affairs, Global Commission on Internet Governance Paper Series 1.

OECD (2018): China's Belt and Road Initiative in the Global Trade. Investment and Finance Landscape, OECD Business and Finance Outlook.

Paris, Roland (2020): The Right to Dominate: How Old Ideas about Sovereignty Pose New Challenges for World Order. *International Organization* 74(3), pp. 453–489.

Prantner, Christoph (2021): China versucht, Deutschland mit der Einheitsfront aufzurollen. *Neue Zürcher Zeitung*, 25 January, https://www.nzz.ch/international/china-rollt-deutschland-mit-der-einheitsfront-auf-ld.1593293 (accessed 24 July 2022).

Robin, Enora / Acuto, Michele (2018): Global Urban Policy and the Geopolitics of Urban Data. *Political Geography* 66, pp. 76–87.

Ruan, Lotus (2019): Regulation of the Internet in China: An Explainer. *The Asia Dialogue*, 7 October, https://theasiadialogue.com/2019/10/07/regulation-of-the-internet-in-china-an-explainer/ (accessed 24 July 2022).

Rühlig, Tim (2020): Technical Standardisation, China and the Future International Order. A European Perspective. Heinrich-Böll-Stiftung, Brussels.

Rühlig, Tim (2022): Chinese Influence through Technical Standardization Power. *Journal of Contemporary China*, https://doi.org/10.1080/10670564.2022.2052439

Rühlig, Tim Nicholas / ten Brink, Tobias (2021): The Externalization of China's Technical Standardization Approach. *Development and Change* 52(5), pp. 1196–1221.

Sadowski, Jathan (2020): Cyberspace and Cityscapes: On the Emergence of Platform Urbanism. *Urban Geography* 41(3), pp. 448–452.

Sassenrath, Henning (2019): "Smart Citys" im Ruhrgebiet: Huawei arbeitet längst an Deutschlands Infrastruktur mit. *Frankfurter Allgemeine*, 27 March, https://www.faz.net/1.6109470 (accessed 24 July 2022).

Schindler, Seth / DiCarlo, Jessica / Paudel, Dinesh (2022): The New Cold War and the Rise of the 21st-century Infrastructure State. *Transactions of the Institute of British Geographers* 47(2), pp. 331–346.

Seaman, John (2020): China and the New Geopolitics of Technical Standardization. The French Institute of International Relations, https://www.ifri.org/en/publications/notes-de-lifri/china-and-new-geopolitics-technical-standardization (accessed 24 July 2022).

Segal, Adam (2020): China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace. In: Nadège Rolland (ed.): *An Emerging China-Centric Order. China's Vision for a New World Order in Practice*. NBR Special Report 87. Washington: NBR – The National Bureau of Asian Research, pp. 85–100.

Sharma, Munish (2020): New Internet Protocol: Redesigning the Internet with Chinese Characteristics? Institute for Defence Studies and Analyses, 15 October, https://idsa.in/idsacomments/new-internet-protocol-msharma-151020 (accessed 24 July 2022).

Shen, Hong (2016): China and Global Internet Governance: Toward an Alternative Analytical Framework. *Chinese Journal of Communication* 9(3), pp. 304–324.

Shen, Hong (2021): *Alibaba: Infrastructuring Global China*. New York: Routledge.

Shen, Yi (2016): Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review* 1(1), pp. 81–93.

Sheng, Jiang (2019): New IP Networking for Network 2030. International Telecommunication Union, https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20191014 16/Documents/Sheng_Jiang_Presentation.pdf (accessed 24 July 2022).

Smart City Duisburg (2018): Duisburg auf der CEBIT. Smart City Duisburg, https://www.duisburg.de/microsites/smartcityduisburg/news/cebit.php (accessed 24 July 2022).

Stabsstelle Digitalisierung (2019): Smart City Duisburg: Masterplan Digitales Duisburg. Stadt Duisburg, 30 September, https://www.duisburg.de/microsites/smartcityduisburg/digitales_duisburg/smart-city-duisburg.php.media/89106/Masterplan_Digitales_Duisburg_-_DIGITAL.pdf (accessed 24 July 2022).

Stadt Duisburg / Huawei (2017): Absichtserklärung. "Memorandum of Understanding" mit der Huawei Enterprise Business Group. Frag den Staat, https://fragdenstaat.de/dokumente/3933/ (accessed 24 July 2022).

Stadt Duisburg (2018): Duisburg wird zur Smart City: Stadt Duisburg und Huawei vereinbaren strategische Zusammenarbeit. Stadt Duisburg, 12 January, https://duisburg.de/guiapplications/newsdesk/publications/Stadt_Duisburg/102010100000062261.php (accessed 24 July 2022).

Stadt Duisburg (2019a): Smart City Duisburg. Stadt Duisburg, https://www.duisburg.de/microsites/smartcity-duisburg/informationen_downloads_/informationen-downloads.php.media/84061/Smart_City_Duisburg_english-Website.pdf (accessed 24 July 2022).

Stadt Duisburg (2019b): Beschlussvorlage 19-0883. 2 September, https://sessionnet.krz.de/duisburg/bi/vo0050.asp?__kvonr=20086242 (accessed 24 July 2022).

Stadt Duisburg (2021): Jahresübersicht über die steuerungsrelevanten Beteiligungsunternehmen der Stadt Duisburg. Berichtsjahr 2020. Stadt Duisburg, 31 December, https://www.duisburg.de/vv/produkte/pro_du/dez_i/20/jahresuebersicht.php.media/137189/JUe-2020.pdf (accessed 24 July 2022).

SAC – Standardization Administration of China (2020): Main Points of National Standardisation Work in 2020 (2020年全国标准化工作要点). Standardization Administration of China, Issue 8.

Star, Susan Leigh / Ruhleder, Karen (1996): Steps toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. *Information Systems Research* 7(1), pp. 111–134.

Stern, Rachel E. / Kim, Jieun / Liebman, Benjamin L. (2022): Performing Legality: When and Why Chinese Government Leaders Show Up in Court. Fairbank Center for Chinese Studies, https://cscc.sas.upenn.edu/events/2022/04/08/performing-legality-when-and-why-chinese-government-leaders-show-court (accessed 24 July 2022).

The Ministry of Foreign Affairs and the Cyberspace Administration of China (2017): International Strategy of Cooperation on Cyberspace. 1 March, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/201703/t20170301_599869.html (accessed 24 July 2022).

The National Development and Reform Commission of China (2018): Action Plan on Belt and Road Standard Connectivity (2018–2020). 11 January, https://www.yidaiyilu.gov.cn/zchj/qwfb/43480.htm (accessed 24 July 2022).

The State Council of the People's Republic of China (2021): China Issues Outline to Promote Standardized National Development. The State Council of the People's Republic of China, 11 October, http://english.www.gov.cn/policies/latestreleases/202110/11/content_WS616370f4c6d0df57f98e1758.html (accessed 24 July 2022).

Tomlinson, John (1999): *Globalization and Culture*. Chicago: University of Chicago Press.

Triolo, Paul / Allison, Kevin / Brown, Clarise (2020): *The Digital Silk Road: Expanding China's Digital Footprint*. New York: Eurasia Group.

Triolo, Paul / Greene, Robert (2020): Will China Control the Global Internet via Its Digital Silk Road? *SupChina*, 8 May, https://supchina.com/2020/05/08/will-china-control-the-global-internet-via-its-digital-silk-road/ (accessed 24 July 2022).

Van der Vleuten, Erik (2004): Infrastructures and Societal Change. A View from the Large Technical Systems Field. *Technology Analysis & Strategic Management* 16(3), pp. 395–414.

Velliet, Mathilde (2022): Convince and Coerce. U.S. Interference in Technology Exchanges Between its Allies and China. The French Institute of International Relations, https://www.ifri.org/sites/default/files/atoms/files/velliet_convince_coerce_united_states_china_2022.pdf (accessed 21 July 2022).

Vila Seoane, Maximiliano Facundo (2020): Alibaba's Discourse for the Digital Silk Road: The Electronic World Trade Platform and "Inclusive Globalization". *Chinese Journal of Communication* 13(1), pp. 68–83.

Wang, Xiaosong (2020): New Infrastructure Can Boost Economy. *China Daily*, 14 May, https://global.chinadaily.com.cn/a/202005/14/WS5ebc85c0a310a8b241155809.html#:~:text=At%20present%2C%20it%20mainly%20includes,and%20development%20for%20public%20benefit (accessed 24 July 2022).

Wang, Yi / Gray, Joanne E. (2022): China's Evolving Stance against Tech Monopolies: A Moment of International Alignment in an Era of Digital Sovereignty. *Media International Australia* 185(1), pp. 79–92. https://doi.org/10.1177/1329878X221105124

WAZ (2019): Chinesischer IT-Riese Huawei ist für Duisburg ein Risiko. *Westdeutsche Allgemeine Zeitung*, 24 May, https://www.waz.de/staedte/duisburg/chinesischer-it-riese-huawei-ist-fuer-duisburg-ein-risiko-id22-1223665.html (accessed 24 July 2022).

Wong, Chunhan (2020): China Launches Initiative to Set Global Data-Security Rules. *The Wall Street Journal*, 8 September, https://www.wsj.com/articles/china-to-launch-initiative-to-set-global-data-security-rules-11599502974 (accessed 24 July 2022).

World Bank Group (2019): Infrastructure Connectivity, Japan G20 Development Working Group. World Bank Group, https://www.oecd.org/g20/summits/osaka/G20-DWG-Background-Paper-Infrastructure-Connectivity.pdf (accessed 24 July 2022).

Wu, Jun / Wan, Qingqing (2014): From WeChat to We Fight: Tencent and China Mobile's Dilemma. PACIS 2014 Proceedings, p. 265. AIS eLibrary, http://aisel.aisnet.org/pacis2014/265 (accessed 24 July 2022).

Wu, Tim (2020): A TikTok Ban is Overdue. *The New York Times*, 18 August, https://www.nytimes.com/2020/08/18/opinion/tiktok-wechat-ban-trump.html (accessed 24 July 2022).

Xi, Jinping (2015): Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference. Ministry of Foreign Affairs of the People's Republic of China, https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html (accessed 24 July 2022).

Xi, Jinping (2017): Work together to Build the Silk Road Economic Belt and the 21st Century Maritime Silk Road. Opening speech, The Belt and Road Forum for International Cooperation, 14 May, Beijing.

Zeng, Jinghan / Stevens, Tim / Chen, Yaru (2017): China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". *Politics and Policy* 45, pp. 432–464.

Zhang, Chong (2020): Who Bypasses the Great Firewall in China? *First Monday* 25(4). https://doi.org/10.5210/fm.v25i4.10256

Zhang, Phate (2020): Huawei Rotating Chairman: New IP is a Purely Technical Subject. CNTechPost, 3 April, https://cntechpost.com/2020/04/03/huawei-rotating-chairman-new-ip-is-a-purely-technical-subject/ (accessed 24 July 2022).

Zhao, Bo / Feng, Yang (2021): Mapping the Development of China's Data Protection Law: Major Actors, Core Values, and Shifting Power Relations. *Computer Law & Security Review* 40(105498), pp. 1–60.

Zhu, Julie / Yang, Yingzhi / Wu, Kane (2022): China Fines Didi $1.2 bln but Outlook Clouded by App Relaunch Uncertainty. Reuters, 21 July, https://www.reuters.com/technology/china-fines-didi-global-12-bln-violating-data-security-laws-2022-07-21/ (accessed 25 July 2022).