Centrality and power: The struggle over the techno-political configuration of the Internet and the global digital order

Pohle, Julia; Voelsen, Daniel

Received: 30 September 2021 | Accepted: 1 March 2022

DOI: 10.1002/poi3.296

RESEARCH ARTICLE

P&I Policy & Internet | PSO | WILEY

Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order

Julia Pohle[1] | **Daniel Voelsen**[2]

[1]Research Group Politics of Digitalization, WZB Berlin Social Science Center, Berlin, Germany

[2]Global Issues Research Division, German Institute for International and Security Affairs, Berlin, Germany

Correspondence

Julia Pohle, Research Group Politics of Digitalization, WZB Berlin Social Science Center, Reichpietschufer 50, Berlin 10785, Germany.
Email: julia.pohle@wzb.eu

Daniel Voelsen, Global Issues Research Division, German Institute for International and Security Affairs, Berlin, Germany.
Email: Daniel.Voelsen@swp-berlin.org

Abstract

In recent years, various governments have been trying to subordinate the Internet to the system of the Westphalian state order. This article seeks to add a new layer to the analysis of this conflict over state sovereignty and the global digital order. It draws on network theory as an alternative analytical lens to study the reconfiguration of power relations that define the Internet as a technical, social and economic network, and its governance. We review key conflicts and developments that shaped the Internet's history, from the Internet exceptionalists' visions in the 1990s to states' recent pursuits of digital sovereignty and trace how states, as well as private companies, seek to fundamentally reconfigure the dominant logic of the Internet and its sub-networks to expand and institutionalise their power position. We thus highlight a deeper layer of conflict: the current struggles over the techno-political configuration of the Internet are not only influenced by the conflict between liberal and authoritarian visions of the Internet; they are also the result of continuous tensions between processes of centralisation and decentralisation of the Internet's technical foundations and its governance. As an effect of these dynamics, we currently witness a pluralisation of power while, at the same time, new points of centralised control emerge.

[Correction added on 29 March 2022, after first online publication: Title has been updated from "The struggle over the techno-political configuration of the Internet and the global digital order" to "Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order" has been added.]

KEYWORDS
digital economy, digital sovereignty, fragmentation, Internet governance, network, power

INTRODUCTION

It is hard to imagine globalisation without the Internet. The originsof globalisation processes—understood as the increasingly dense interweaving of societies beyond local and regional contexts—go back much further than the invention of the Internet. Yet, with the spread of the commercial Internet since the 1990s, there has been a leap in global flows of communication and information. From global trade to the realm of personal relationships, an increasing number of today's social interactions rely on the exchange of large amounts of digital data, at vanishingly low cost and in near real-time. The Internet is the infrastructure that underpins these globalisation processes and the core of the global digital order. This global digital order is the sum of technical, economic, political and regulatory practices that determine the worldwide information flows. Governments, private companies and civil society actors continuously shape and reshape the contours of this order.

The Internet does not prescribe only one particular global digital order. How the Internet is used, and what kind of social and economic relationships it is supposed to foster, has always been contingent and politically contested. Especially in the early days, the spread and use of the Internet was accompanied by diffuse cosmopolitan expectations and utopian ideas of a virtual, networked world community (Barlow, 1996; see also Chenou, 2014, pp. 212–215). In recent years, however, we can observe a return to the established patterns of the Westphalian state system: with different political thrusts, authoritarian as well as liberal governments increasingly seek to assert state sovereignty on and through the Internet. These attempts are commonly described as a geopolitical conflict between a liberal and an authoritarian vision of the Internet, fought out between states and transnational actors. Among cosmopolitans, this development has triggered concerns about a "fragmentation" of the Internet (Drake et al., 2016; J. F. Hill, 2012; Mueller, 2017). The term "fragmentation" suggests an image of a formerly homogeneous, intact structure, which disintegrates and splits into national Internet segments that can no longer interact smoothly with each other. Yet, this fear and its underlying idea of a previously homogeneous structure not only ignores the fact that almost half of humanity still has no access to the global Internet, but it also denies the many regional differences in the use, design and regulation of the Internet and its applications.

In this study essay, we aim to add another layer to the analysis of the supposed fragmentation of the Internet and the restrictive binary interpretation of ongoing tensions as a geopolitical conflict between liberal and authoritarian states. Taking inspiration from network theory and its conception of power, we analyse how different attempts to exercise power within and over networks have shaped the Internet's development over the last decades. This analysis also shows that the current struggles over the techno-political configuration of the Internet as a technical, social and economic network represent the confrontation of different visions of how centralised, or decentralised, the Internet and, more generally, the global digital order should be. This analytical approach provides a new perspective as it can explain why it is unlikely that ongoing attempts by governments as well as major private companies to assert their power will lead to the complete loss of a global digital infrastructure for the exchange of communication and data. Rather, as we argue, these actors seek to fundamentally reconfigure the dominant network logic of the Internet: their goal is to subordinate particular subnetworks to a more centralised logic

and, at the same time, expand and institutionalise their power position within these networks.

Drawing from a broad range of research literature and the empirical and theoretical findings therein, we seek to understand these political dynamics through a historical perspective.[1] Starting with the US influence on the Internet's origins, we focus on key conflicts and developments to retrace how influential actors have continuously reconfigured its underlying network structure on a technical and a political level. We thereby regard both the layer of the Internet's basic infrastructure and the layer of Internet applications.[2] We then analyse the ongoing efforts by states—primarily China and Russia but also a number of democratic countries—to counter the US dominance and the more recent efforts of private companies to expand their power over certain parts of the network, as well as the global network as a whole. As an effect of these efforts, we argue in the conclusion, we can observe a pluralisation of power whereby the influence of the United States is reduced; at the same time, new points of centralised control emerge.

THE INTERNET AND THE LOGICS OF NETWORKS

Social science research has long tended to view the Internet—and technology in general—as a given artefact; the focus was on the disruptive power and the transformations triggered by the rise of the Internet. In recent years, however, the Internet has increasingly been conceptualised not only as a driver of social and political processes but also as their product, leading to a growing interest in how technology, politics, and society co-constitute each other (Berg et al., 2020). This development is due not least to the increasing popularity of interdisciplinary fields of study, such as science and technology studies, and the return to the foundations of social constructivism and the sociology of technology (DeNardis, 2014; Epstein et al., 2016). This new stream of research often focuses on the contingency of social and technological developments. In this spirit, David D. Clark, an American computer scientist and one of the early architects of the Internet infrastructure, has called for the entire history of the Internet's development to be understood as essentially contingent: "to recognize that there were multiple options for the early Internet, and that the Internet as we know it is contingent on decisions that could have led to different outcomes, is to recognise that the future of the Internet is itself contingent" (Clark, 2016, p. 9).

This article builds on such an understanding of the contingency, and the mutual co-constitution, of technological, social, economic and political processes. To this end, it approaches the Internet's development through a network-theoretical perspective. It is common to view the global Internet as a network of networks, that is, a complex system of numerous interconnected subnetworks of different sizes and shapes. Thus understood, the Internet holds the potential for a decentralised structure that avoids the concentration of political as well as economic power, and only requires a few points of coordination and contact.[3] Equally conceivable, however, is a network structure that creates centralised power positions. The history of the Internet, then, can be understood as an ongoing conflict over its network configuration. The Internet started out as a mostly decentralised network. Over the last three decades, however, powerful states, and increasingly also powerful transnational companies,[4] have taken different steps to consolidate their power within the Internet and its different subnetworks, sometimes even going so far as attempting to reconfigure the certain subnetworks, or even the entire network of the Internet.

To analyse these processes of network reconfiguration, we take inspiration from the way in which network theory conceptualises power relations (Castells, 1996, 2016, p. 12; Kahler, 2009).[5] This relates, first, to *power within networks*, for which the centrality of actors' positions in existing networks is particularly decisive. A central position in a network is defined by a

higher number of connections to other entities in this particular network. Compared to entities on the periphery of the network, central actors have more options for action and, thus, ultimately more power. For example, they can act as "gatekeepers" for particular networks, controlling access to certain goods or services (Goddard, 2009, p. 257). Crucially, however, these actors do not have the power, or even the ambition, to fundamentally change the way in which the network functions. A second form of network-related power is *power over networks*, understood as the ability to fundamentally change the structure of a network, including the power to decide whether and under what conditions connections to other subnetworks are established. Essentially, power over networks means control over the logics of networks, including the ways in which power is distributed within these networks (Zajacz, 2019, p. 27). This kind of power can, in principle, be exercised both at the level of the global network as well as at the level of subnetworks. An entity holding *power over* a network can make use of it to create for itself a centralised position of *power within* the network. Power over a network, thus, often goes hand in hand with power within the same network.

It is often assumed that networks are designed in a decentralised way, such that no entity can occupy a central position of power within the network. This assumption, in turn, is generally linked to normative expectations about networked forms of organisation. In particular, in the field of Internet governance, a decentralised and nonhierarchical network is often understood as a favourable alternative to traditional forms of social organisation (Lambach, 2020, 485; Mueller et al., 2013, p. 87). Network organisations are considered as more open, flexible and inclusive than traditional forms of organisation—for instance, the family or the nation. Moreover, unlike hierarchical forms of governance, networks are often associated with forms of voluntary and cooperative coordination (August, 2021; Pohle & Thiel, 2019, p. 62). However, it is important to note that networks can also be designed in a way that allow central positions and opportunities for the exercise of power within the networks. For our analysis, it is useful not to presume the configuration of the Internet by ascribing normative meanings to the concept. Instead, we make the nature of the network itself the object of investigation. The question of how centralised or decentralised the Internet should be, is about the character of the technical, social, economic and political subnetworks which, in their entirety, constitute the global Internet.

The struggle for the future of the Internet is often portrayed as a geopolitical conflict between liberal and authoritarian states. Our approach unearths a deeper layer of confrontation. Underneath the ideological divergence, we can observe a conflict over centrality and power in networks. This conflict goes beyond the traditional forms of geopolitics and does not neatly correspond to the patterns of the liberal-authoritarian dichotomy. Democratic governments, as well as companies headquartered in Western democratic countries, likewise pursue efforts to create, and occupy, central positions of power with regard to subnetworks of the Internet or the Internet as a whole. On this level, their goals are not very different from those of authoritarian governments. One might say, thus, that by seeking to institutionalise their power *over* and *within* networks, liberal actors unwittingly and inadvertently contribute to establishing centralised network structures that are particularly well suited for the needs of authoritarian governments. In sum, these developments culminate in the trend towards a global digital order that is both more centralised and more authoritarian than in the past.

THE INTERNET'S ROOTS IN AMERICAN LIBERALISM

From the 1960s onwards, there have been attempts in various countries to connect the computer systems of different research institutions. The most comprehensive network of this kind was ARPANET, a system sponsored by the US Department of Defense (Abbate, 1999).

Although the Internet as we know it today did not establish itself as the dominant global network for data exchange until the early 1990s, many of the technical standards and protocols that are of fundamental importance for the exchange of data on the Internet were developed in the first decades of its existence. These standards and protocols that have influenced the way societies perceive, and use, the Internet to this day. On a technical level, they represent the idea of a deliberately open and decentralised network configuration. The basic web and email protocols are prime examples: A website can be read on different devices and the common set of protocols allows compatibility between different service providers. Users can thus choose from a variety of providers to host websites and use email without losing connectivity to the broader network (Arkko, 2020; Masnick, 2019).

Yet, even at this stage of its development, the Internet also exhibited certain features of centralisation of power. First, it was the early Internet infrastructure itself that was, to some extent, centrally organised. For example, the domain name system (DNS)—also known as the Internet's address book because it maps human-readable web addresses onto computer-readable IP addresses—was initially managed by one person, Jon Postel, an American computer scientist and Internet pioneer. Officially, this task fell to the Internet Assigned Numbers Authority (IANA), which was originally overseen and funded under the authority of the US Department of Defense. In practice, however, it was Postel who assigned addresses to new subscribers and added them to the network. Thus, with this privileged position of power within the network, Postel and IANA were in a position to act as gatekeepers who could, in principle, deny new providers of websites access to the Internet (Ahlert, 2001, p. 70)—though there are no reports of any instances in which this power was actually exercised.

Second, the early political economy of the Internet also established central actors with regard to both the infrastructure and the application layer of the Internet. Initially, the Internet as a US project was promoted by massive public investment (Mazzucato, 2013, p. 80); the use of the networks for commercial transactions was not permitted. This changed in the 1990s when the Clinton administration pursued a policy of deliberate privatisation and commercialisation of the Internet. Internet access became a commodity and private companies began to expand the Internet's infrastructure (Radu, 2019, p. 75).[6] As a result, today a large part of the Internet infrastructure in the United States and many other countries that emulated its policy approach is in the hands of private companies. In this sense, the global Internet was a child of its time—it was shaped by neo-liberal notions of the superiority of markets over public institutions (Chenou, 2014). But while this commercialisation led to the Internet's global expansion and paved the way for innovations that continue to define its use, it also led to a concentration of the Internet's infrastructure in the hands of a few US providers, giving them an important position of power within the global network of the Internet. For instance, by 1995 Netscape Navigator, one of the first commercial web browsers, was by large the most widely used web browser and thus represented the gate to the World Wide Web for the bulk of Internet users worldwide. It later had to cede this power position to Microsoft's Internet Explorer which attained more than 90% usage share around the year 2000.

US policy, however, did not just impact the early digital economy. More broadly, it is probably the most profound example of power over the global network in that it shaped the Internet in line with broadly liberal principles—while securing a central position of power for the US government. The early structures of global Internet governance exemplify this twofold strategy. In 1998, the Internet Corporation for Assigned Names and Numbers (ICANN) was founded with the aim of providing an institutional framework for the IANA functions carried out by Postel. ICANN's newly created working and decision-making structures were geared to the criteria of self-regulation and multi-stakeholder governance. The hope behind this governance model was—and remains until today—to facilitate voluntary cooperation among all those who have a stake in the Internet and its future development, from end-users to civil society and private companies; while government

representatives are also included, they are denied any kind of privileged position of power (Hofmann, 2016). The primarily US-driven idea that a multi-stakeholder governance model would be most adequate for the global Internet was further institutionalised through the creation of the Internet Governance Forum (IGF). Like ICANN, the creation of the IGF was supported by the US as it sought to assure a context for international discussion on Internet-related issues that does not prioritise hierarchical or governmental decision-making. Yet, at the same time, the US government secured a privileged position of power for itself in the early institutional structures for the governance of the global Internet, most prominently by giving its own Department of Commerce oversight over IANA's functions (Weinberg, 2011). ICANN, in particular, can thus be seen as an emblematic example of the kind of global digital order sought by the US government. It combined liberal ideas of order and an emphatic commitment to the idea of multi-stakeholder governance with the attempt to preserve the central position of both the US government and US companies. From the US perspective, this was not understood as a contradiction; rather, it was the strong and central position of the United States that allowed it to be seen as a guarantor of a liberal digital order. Not surprisingly, however, the founding of ICANN—which reinforced the US *power over the network* of the global Internet—and the IGF—which institutionalised the idea of denying governments an exclusive decision-making power over the Internet and, hence, was thought to contribute to a more decentralised governance structure—was met with continuing resistance from all those governments that were relegated to the periphery of the network and did not subscribe to this notion of the liberal order, most importantly by authoritarian countries such as Russia and China (Nocetti, 2015, p. 117).

THE DUALITY OF GLOBAL DECENTRALISATION AND LOCAL CONCENTRATIONS OF POWER

In the following years, these struggles about the global Internet and its governance continued. Indeed, as Internet use grew and diversified, so did the awareness on the part of many states that they were increasingly dependent on digital infrastructures and their applications. Ever since ICANN's foundation in 1998, there had been several attempts by authoritarian countries to mobilise other states to move against the privileged position of the US government with regard to the Internet core infrastructures, most notably during the World Summit on the Information Society (WSIS), a United Nations' conference that took place in 2003–2005 (Kleinwächter, 2004) and resulted in the creation of the IGF and the institutionalisation of a multi-stakeholder setting for debates about the global Internet and its governance. In 2012, this latent conflict in global Internet governance had escalated to such a point that observers were talking about a "digital cold war" (R. Hill, 2013; Musiani & Pohle, 2014). At the World Conference on International Telecommunications (WCIT), a number of states, led by Russia, insisted once again that—instead of ICANN—an intergovernmental institution, more specifically the International Telecommunication Union (ITU), should be responsible for managing the Internet's address system (Kennedy, 2013, p. 16). The stated goal was to strengthen the position of governments in global Internet governance by essentially giving them complete power over, and then also within "their" national subnetworks—and at the same time weaken the United States power over the global network by transferring control over the DNS from ICANN to the ITU. Although the United States and its allies were able to prevent this coordinated attempt to reconfigure the political structures of Internet governance, the conflict has continued to smoulder ever since. In the following, we analyse key events that illustrate the attempts of actors to establish new power positions and how they resulted, in many instances, in the pluralisation of power and, at the same time, led to a more centralised network logic.

Control over the Internet's global infrastructure

In the summer of 2013, the political dispute over the Internet's global infrastructure was exacerbated by Edward Snowden's leaking of internal documents from the US National Security Agency (NSA), which disclosed the enormous extent to which US authorities and intelligence agencies monitored and analysed Internet data traffic worldwide. The leaks revealed a well-established practice of the US government using the data collected by major US tech companies about their users. Many of the companies implied in this practice criticised the way in which the government had instrumentalised them. Yet, what they could not deny were the similarities between the surveillance practices of the intelligence services and the business models of the big tech companies—which explain why the data collected by these companies is so attractive for governments all around the world (Zuboff, 2018). In addition, US intelligence agencies relied on cooperation with partner agencies in Europe and other Western states to access global data flows (Bauman et al., 2014).

The Snowden revelations confirmed warnings by those who had even before harboured concerns about the power of the United States over the Internet's global infrastructure, as manifested in its influence on ICANN and the dominance of US companies. Although the disclosures were followed by surprisingly little concrete political counteractions (Steiger et al., 2017; Tréguer, 2017), the public and political outcry that followed the release of the documents made clear that they had initiated a shift in awareness. Even states that saw themselves as supporters of the existing global digital order were now concerned that the US government and US companies were exploiting their almost hegemonic position of power (Farrell & Newman, 2019; Ni Loideain, 2015). Thus, the Snowden revelations also prompted what was perhaps the most ambitious call to break the predominance of US control on Internet infrastructure: the Global Multistakeholder Meeting on the Future of Internet Governance, also called NETmundial, hosted by the Brazilian government in 2014. The meeting, which can also be interpreted as a critique of the actual effectiveness of multi-stakeholder "pioneers" like the IGF, developed a shared set of Principles and a Roadmap, which however had very little long-lasting impact (Musiani & Pohle, 2014).

One US response to the mounting international criticism and the NETmundial meeting was to relinquish nominal control over IANA and its responsibilities regarding the Internet's address system. Following a process that took several years, in 2016 oversight over IANA's functions was eventually handed over to a newly created multi-stakeholder structure within ICANN. While many Western governments actively supported this transition, other states—notably Russia and Brazil—criticised the great influence of US companies in ICANN and the fact that ICANN, as a Californian company, remained within the jurisdiction of the United States. Indeed, while the inclusion of more actors through ICANN's multi-stakeholder mechanisms potentially resulted in an even more decentralised governance structure, the United States retained a central position of power over the DNS, a core component of the Internet's global infrastructure. This became visible when, in 2018, the Trump administration floated the idea of reversing the IANA transition (Mueller & Kane, 2018). Eventually, this plan did not materialise—but for many states worldwide, this episode highlighted that, in principle, the US government could, at any point in time, assert control over IANA and, thereby, the global DNS.

In sum, many state and non-state actors made efforts to reduce power imbalances at the level of the Internet's global infrastructure and its core governance mechanisms. The US, however, retained a central position of power. The early imaginary of the Internet as a truly decentralised, open network with a global reach still held a lot of attraction but already turned out be to more difficult to achieve than expected.

Liberal and authoritarian practices of digital sovereignty

Despite the backlash provoked by the Snowden leaks, the power relations on the scale of global network did not change substantially over the last decades. Yet, if we go beyond the core global infrastructures such as the DNS and view the global network as an amalgamation of subnetworks, seismic shifts can be observed. Already starting in the late 1990s, several states began to reassert control over their national digital infrastructures. Emphasising their ambition to strengthen their own "digital sovereignty," they chose a path that required little coordination with the global network structures controlled by the US government and US companies.

The Russian state's efforts are particularly far-reaching. At the end of 2019, the Putin government announced a package of measures that aimed to establish a "sovereign Internet", including technical measures designed to territorialise information flows as well as compelling Russian Internet providers to create the technical infrastructure to allow all Internet traffic to be routed locally, if deemed necessary by the government. The stated goal is to expand the Russian government's power over and within the Russian subnetwork of the Internet. Indeed, the Russian government even seeks control over the DNS to no longer depend on ICANN (Epifanova, 2020; Soldatov, 2019), which represents an emblematic example of a state seeking power over "its" network in a way that effectively impacts the global network's configuration. This extreme case of power over a subnetwork, thus, also includes an element of power over the global Internet.

China's government has already achieved the goal of securing for itself a central position of power within and the full control over the Chinese Internet. Situated in an authoritarian political system, the resulting network configuration is aptly described as "networked authoritarianism" (MacKinnon, 2011). In addition to its domestic efforts, next to Russia, China is one of the few countries in the world that is proactively attempting to reshape the global digital order. The Chinese political leadership sees the Internet, and digital technologies more broadly, as an opportunity to greatly accelerate the country's economic development and to expand the Chinese government's influence beyond the country's borders. Its declared ambition is to become a "cyber superpower" on a global scale (Arsène, 2016), establishing itself as a central actor holding power over many parts of the global Internet. The underlying strategic thinking is similar to that of the United States: like the US, China seeks to achieve political and economic superiority through technological "supremacy" (Schulze & Voelsen, 2020).[7] This is being practically implemented in the extensive efforts to develop and disseminate technical standards (Rühlig, 2020) and the large number of digital infrastructure projects in Asian and African countries as part of the "Belt and Road Initiative" (BRI) (Eder et al., 2019). China, like Russia, is also actively seeking to influence relevant discussions on digital governance issues within the framework of the United Nations (Flonk, 2021); moreover, China has held the directorship of the ITU for several years.

But the pursuit of sovereignty in the digital sphere is not limited to authoritarian countries, although it started there much earlier. Several democratic states also seek to assert their political, economic and social self-determination with regard to digital technology. This should not come as a surprise since liberal democracy embodies the ideal of collective self-determination, which in turn requires the institutional capacity to reign over developments that affect one's society. In Europe, for instance, both France and Germany are very outspoken about their ambition to strengthen their own digital sovereignty as well the one of the European Union more generally (Danet & Desforges, 2020; Pohle, 2020). They, too, wish to expand the power they have over their national subnetworks, although with a less holistic ambition than authoritarian countries. Instead of seeking control over their population or a complete independence of "their" national subnetworks, their claims and actions are motivated by their wish to limit the power of the US government that became visible through the Snowden leaks in 2013 as well as the power of the big tech companies in today's platform

economy. While in many ways the US is still their closest ally, democratic countries—in particular in Europe—emphasise their wish to shape a digital order based on their own values and ideas, domestically and on the global level. To this end, for example, they implement cyber security policies to protect critical data and technical infrastructures. In addition, they seek to strengthen their own digital markets through regulatory policies and by actively promoting digital skills and competences.

In sum, the efforts of both authoritarian and democratic states to reassert their sovereignty over the Internet constitutes a trend towards a reconfiguration of the Internet, in which the United States still maintains control over certain core infrastructures, while at the same time governments exert ever greater power over and within their national subnetworks. While their efforts result in new points of central control within these subnetworks, this diversification of power on the global level leads to a more decentralised network structure for the Internet as a whole. What is more, on the level of the subnetworks, thus, we now see more political plurality: Whereas initially the national networks mostly followed the template of the US Internet, a growing number of states configure their national networks in line with their political goals and traditions and thereby rewrite the internal logics of these networks.

Power in the digital economy

Parallel to the trend of an increasing political pluralisation and decentralisation of the global digital order, the last decade also witnessed a considerable trend towards concentration of power in another domain: in an increasingly integrated global digital economy, a number of technology companies succeeded in exploiting the scale and network effects of the Internet. Most prominently, big US tech companies such as Google, Apple, Facebook, Amazon and Microsoft (in short: "GAFAM") hold a central position of power within the networks that shape the application layer of the Internet in many parts of the world. At the moment the only real competition on a global level comes from Chinese companies like Baidu, Alibaba and Tencent—which also have been assigned an acronym, "BAT" (Jolly, 2021; Seoane, 2019).

This concentration of power has repercussions for the structures of the Internet as a network. Regarding the infrastructure level of the Internet, companies from the United States as well as from China are seeking to secure their central position by investing heavily in the development of technical standards (ten Oever, 2021, p. 346) and in the construction of their own physical infrastructures—from data centres to underwater cables (Lehr et al., 2019; Mauldin, 2017; Winseck, 2017, p. 262). On this infrastructure level, these companies hold power over the global Internet on a level that exceeds that of most of the countries in the world. At the application level, these tech giants seek to create subsystems within the Internet that are self-contained, and thus protected from competition. Seen through the lens of network theory, these companies are attempting to turn their "platforms" (operating systems, social networks, trading centres, app stores) into distinct subnetworks, within which they can occupy central positions of power.

But the recent trend towards a "platformisation" of the digital economy not only impacts the network configuration of the digital economy. The concentration of power over the digital public sphere in the hands of a few corporations is also influencing the communication and behaviour of Internet users. In many Western countries, the dominant media platforms are operated by US tech companies such as Meta Platforms (Facebook, Instagram and WhatsApp) or Alphabet (Google); in other parts of the world, Chinese platforms such as WeChat or the Russian service Telegram have assumed a central position. These media platforms can be understood as another type of subnetworks. Because these subnetworks are creations of the operators behind them, the companies hold enormous power within these networks. The platforms act as intermediaries that, as classic gatekeepers, use their algorithms and terms of service to determine which content can be found, seen and

perceived by which users. The rules on how and under what conditions users can exchange information via these central platforms are therefore set by the operators themselves and are only changed under great pressure from users or states (Gorwa, 2021; Katzenbach, 2021). As it is the case for the Russian government's activities, the massive power of these platforms over subnetworks, to a certain degree, also gives them power over the global Internet (Stocker et al., 2021).

The concentration of information and communication flows on the platforms that dominate the digital economy is frequently criticised for leading to an increasing polarisation of the digital public sphere. The reason for this, it is argued, are their underlying business models, which follow the logic of the attention economy (Christl & Spiekermann, 2016; Williams, 2018, p. 17). The mass digital dissemination of disinformation and hate speech through channels without the content control mechanisms of traditional mass media—combined with political polarisation through the selective distribution of content thanks to micro-targeting techniques (Christl, 2019)—are just some of the consequences associated with this process. In response to these developments, political decision-makers have come under pressure to regulate digital public spheres and the platforms that enable them. Many countries are still relying on voluntary self-regulation, that is, self-regulation by platform providers, thereby following the policy approach shaped by the United States in the early years of the Internet. Yet, we can also observe an increased tendency, including in democratic countries, to intervene more strongly in Internet users' communication behaviour within privately owned subnetworks. Essentially, this is a conflict over who holds central positions of power within these subnetworks. In recent years, the EU, in particular, has relied on regulation to set standards in Europe and to enforce limits on both domestic and foreign authorities and companies—with several of these measures, such as the General Data Protection Regulation (GDPR) having repercussions on a global scale (Bradford, 2020, p. 20).

In sum, the rise of the platform economy has led to a new level of concentration of economic and social power within the hands of a handful companies. Given the size and growing centrality of company-owned subnetworks, they also affect the larger topology of the Internet as a whole. In addition, by establishing their own rules, powerful platform companies not only define the logic "their" Internet subsections, but they are able to also exercise significant power regarding both the infrastructure and application layer of the global network. Currently, their power and the resulting centralisation of the Internet is limited only by regulatory efforts of both authoritarian and democratic states which seek to assert their own autonomy and—at least some of them—to protect the capacity of self-determination of their citizens vis-à-vis these powerful gatekeepers.

CONCLUSION: TOWARDS AN AUTHORITARIAN RECONFIGURATION OF THE GLOBAL DIGITAL ORDER?

The global disputes over the Internet can be understood as conflicts over the (re) configuration of the network that are occurring along two dimensions. The first dimension concerns the struggle over centralisation versus decentralisation, meaning the question how centralised or decentralised the Internet is organised. This dimension of the conflict is primarily driven by actors who seek to create, or defend, central positions of power over and within the global network. The second dimension concerns political ideologies and the divergences between liberal and authoritarian visions of the Internet, including also those that have elements of both these positions. Here, the existing liberal framework of the global digital order is increasingly challenged by authoritarian efforts to fundamentally rewrite the political logic of the global Internet.

There is an "elective affinity" between a decentralised network configuration that incentivises a wide distribution of power and liberal ideals of setting up various "checks and balances" to restrain the exercise of power. On the other end of the spectrum, a strongly centralised network configuration fits well with the logic of authoritarian rule. However, these are not the only possible combinations of the two dimensions of the conflict about the future of the global Internet and the global digital order. The idea of centralised hierarchy is certainly familiar to liberal notions of legitimate authority. Likewise, a "smart" authoritarian leader can use a certain degree of decentralisation to stabilise its claim to power. As a consequence, we are confronted with a complex, multidimensional conflict. Our analysis of this two-dimensional conflict also sheds new light on the debate about the fragmentation of the global Internet. What we are witnessing is indeed a trend towards a more pluralistic topography of the global Internet. Where once the US provided the blueprint for almost all subnetworks worldwide, today we see many governments contributing to an increasingly diverse set of rules for the global Internet through regulation, thereby actively shaping their national subnetworks in ways that depart from the US model. Major technology companies, moreover, create their own subnetworks under their corporate control—sometimes euphemistically called "eco-systems"—which are governed by their own rules and the requirements of the underlying business models. What all these efforts have in common, despite their varying political or economic goals, is the attempt to centralise power and control over what they perceive as "their" networks. This trend towards a more pluralistic global Internet, however, is unlikely to reach the point where the Internet as a whole fragments into different Internets (Mueller, 2017). All those actors seeking to consolidate power over, and within, their subnetwork have a strong incentive to be able to connect with other subnetworks. From the perspective of network theory, it is not in the best interest of any of these actors to cut all connections or completely prevent data exchange between the network they control and other networks on the Internet. Instead, these actors seek to control how "their" subsystem of the Internet connects to the rest of the network, what kind of data can be exchanged and under what conditions.

Nonetheless, our analysis leads to a sober prospect for the future of the global Internet and the global digital order in general. It can be expected that there will be a consensus for maintaining the common foundation or public core of the global Internet. Yet, this consensus will likely be limited to the functional requirements of global coordination that all actors can agree on; it will not necessarily include more contentious political issues such as free speech or fair, market-based competition. If, then, within this thin global framework, authoritarian forms of Internet governance spread further, we may face a gradual reconfiguration of the global digital order "from below" (Shahbaz & Funk, 2021). In other words: if, at some point in the not-so-distant future the majority of subnetworks are politically designed to serve the purposes of authoritarian rulers, this will shape the global Internet as a whole. At this point, the aggregated power over and within subnetworks becomes power over the network as a whole.

Today, we are at a crossroad. Whether the trend towards a more authoritarian global digital order will continue or even intensify, cannot be predicted. The Internet as we have known it in recent decades has always been contingent—it has been shaped by the decisions of those who developed, used, coordinated and governed it. On the basis of our analysis, it seems that proponents of a liberal Internet should pay more attention to how their actions might lead to a reconfiguration of the Internet and how their efforts to centralise power over and within subnetworks may play into the hands of those actors who wish to overcome what remains of the liberal global digital order.

ACKNOWLEDGMENT

Open Access funding enabled and organized by Projekt DEAL.

ORCID

Julia Pohle https://orcid.org/0000-0002-9442-4626
Daniel Voelsen https://orcid.org/0000-0001-9270-4125

ENDNOTES

[1] Most of the work on the Internet's history is centred around technological developments, paying less attention to the political, social or cultural forces shaping of the Internet (Abbate, 2017; Carr, 2016, p. 14). In addition, these historical accounts often have a US-American focus and ignore "alternative histories" about the evolution of digital networks (Pétin & Tréguer, 2018).

[2] The common distinction between different layers has its origins in the layered architecture typical of networks, which was also used as the basis for the development of the Internet's predecessor, ARPANET. In addition to the "DoD model" originally developed for the US Department of Defense, the so-called TCP/IP reference model is authoritative for the Internet. To reduce complexity, for the purposes of this article we only differentiate between two layers.

[3] The few exceptions, namely central technical control points, enable basic Internet resources to operate—for instance, the root servers of the domain name system. The flat ontology of the network perspective on the Internet can thus certainly be challenged: "not all parts of the Internet are created equal" (Lambach, 2020, p. 489).

[4] While we also consider companies that operate at the level of the Internet infrastructure, for example, by providing Internet access or operating submarine data cables, we primarily focus on those that operate at the level of Internet applications, for example, by providing digital tools and services, such as Alphabet, Facebook or Alibaba.

[5] Castells distinguishes between four forms of power in networks: *networking power*, *network power, networked power* and *network-making power*. The latter form is of particular importance since it is exercised by the actors who can determine the logic of the network (*programmers*) or change the logic of the network (*switchers*); these actors can themselves represent networks (Castells, 2016, p. 12). Our ideas of how power is exercised in networks is inspired by all four forms and takes up the idea of reconfiguring network logics.

[6] The complex history of the commercialisation and privatisation of the Internet has received comparatively little scholarly attention, with a few detailed exceptions (e.g., Greenstein, 2015; Grosse, 2020; McChesney, 2013; Tréguer, 2019).

[7] An unfiltered insight into the Chinese government's strategic thinking is provided by the "International Strategy of Cooperation on Cyberspace" published by the Chinese Ministry of Foreign Affairs in 2017.

REFERENCES

Abbate, J. (1999). *Inventing the internet*. The MIT Press.
Abbate, J. (2017). What and where is the Internet? (Re)defining Internet histories. *Internet Histories*, *1*(1–2), 8–14.
Ahlert, C. (2001). ICANN als Paradigma neuer Formen Internationaler Politik. *Internationale Politik und Gesellschaft*, *1*, 66–78.
Arkko, J. (2020). The influence of internet architecture on centralised versus distributed internet services. *Journal of Cyber Policy*, *5*(1), 30–45.
Arsène, S. (2016). Global internet governance in Chinese academic literature. Rebalancing a hegemonic world order? *China Perspectives*, *2*, 25–36.
August, V. (2021). Technologisches Regieren. Der Aufstieg des Netzwerk-Denkens in der Krise der Moderne. Transcript.
Barlow, J. P. (1996). A declaration of the independence of cyberspace. Electronic Frontier Foundation, February 8. https://www.eff.org/cyberspace-independence
Bauman, Z., Bigo, D., & Esteves, P., et al. (2014). After Snowden: Rethinking the impact of surveillance. *International Political Sociology*, *8*(2), 121–144.
Berg, S., Rakowski, N., & Thiel, T. (2020). Die digitale Konstellation. Eine Positionsbestimmung. *Zeitschrift für Politikwissenschaft*, *30*, 171–191.
Bradford, A. (2020). *The Brussels effect: How the European union rules the world*. Oxford University Press.

Carr, M. (2016). *US power and the internet in international relations: The irony of the information age*. Palgrave Macmillan UK.
Castells, M. (1996). *The rise of the network society*. Blackwell Publishing Ltd.
Castells, M. (2016). A sociology of power: My intellectual journey. *Annual Review of Sociology*, *42*(1), 1–19.
Chenou, J.-M. (2014). From cyber-libertarianism to neoliberalism: Internet exceptionalism, multi-stakeholderism, and the institutionalisation of internet governance in the 1990s. *Globalizations*, *11*(2), 205–223.
Christl, W. (2019). Microtargeting. Persönliche Daten als politische Währung. *Bundeszentrale für politische Bildung*, July 6. https://www.bpb.de/apuz/292349/microtargeting-persoenliche-daten-als-politische-waehrung
Christl, W., & Spiekermann, S. (2016). *Networks of control. A report on corporate surveillance, digital tracking, big data & privacy*. Facultas.
Clark, D. (2016). The contingent internet. *Daedalus*, *145*(1), 9–17.
Danet, D., & Desforges, A. (2020). Souveraineté numérique et autonomie stratégique en Europe: du concept aux réalités géopolitiques. *Herodote*, *177–178*(2), 179–195.
DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.
Drake, W. J., Cerf, V. G., & Kleinwächter, W. (2016). *Internet fragmentation: An overview*. Future of the Internet Initiative White Paper, World Economic Forum.
Eder, T., Arcesati, R., & Mardell, J. (2019). Networking the "Belt and Road"—The future is digital. MERICS (Mercator Institute for China Studies), August 28. https://merics.org/en/tracker/networking-belt-and-road-future-digital
Epifanova, A. (2020). *Deciphering Russia's "Sovereign Internet Law": Tightening control and accelerating the splinternet*. DGAP Analysis, 2. Berlin: Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V. https://www.ssoar.info/ssoar/handle/document/66221
Epstein, D., Katzenbach, C., F., & Musiani (2016). Doing internet governance: Practices, controversies, infrastructures, and institutions. *Internet Policy Review*, *5*(3), 1–44.
Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state Coercion. *International Security*, *44*(1), 42–79.
Flonk, D. (2021). Emerging illiberal norms: Russia and China as promoters of internet content control. *International Affairs*, *97*(6), 1925–1944.
Goddard, S. E. (2009). Brokering change: Networks and entrepreneurs in international politics. *International Theory*, *1*(2), 249–281.
Gorwa, R. (2021). Elections, institutions, and the regulatory politics of platform governance: The case of the German NetzDG. *Telecommunications Policy*, *45*(6), 102145.
Greenstein, S. (2015). *How the internet became commercial: Innovation, privatization, and the birth of a new network*. Princeton University Press.
Grosse, M. (2020). Laying the foundation for a commercialized internet: International internet governance in the 1990s. *Internet Histories. Digital Technology, Culture and Society*, *4*(3), 1–16.
Hill, J. F. (2012). Internet fragmentation highlighting the major technical, governance and diplomatic challenges for U.S. Policy Makers. Policy Report, John F. Kennedy School of Government, Harvard University.
Hill, R. (2013). WCIT: Failure or success, impasse or way forward? *International Journal of Law and Information Technology*, *21*(3), 313–328.
Hofmann, J. (2016). Multi-stakeholderism in internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, *1*(1), 29–49.
Jolly, J. (2021). Is big tech now just too big to stomach? *The Guardian*, February 6. http://www.theguardian.com/business/2021/feb/06/is-big-tech-now-just-too-big-to-stomach
Kahler, M. (2009). Networked politics: Agency, power, and governance. In M. Kahler (Ed.), *Networked politics: Agency, power, and governance* (pp. 1–20). Cornell University Press.
Katzenbach, C. (2021). Die governance Sozialer Medien. In J. H. Schmidt, & M. Taddicken (Eds.), *Handbuch Soziale Medien* (pp. 1–24). Springer VS.
Kennedy, D. (2013). *Deciphering Russia: Russia's perspectives on internet policy and governance*. Global Partners Digital.
Kleinwächter, W. (2004). Beyond ICANN vs ITU? How WSIS tries to enter the new territory of internet governance. *Gazette*, *66*(3–4), 233–251.
Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review*, *22*(3), 482–506.
Lehr, W., Clark, D., Bauer, S., Berger, A., & Richter, P. (2019). Whither the public internet? *Journal of Information Policy*, *9*, 1–42.

MacKinnon, R. (2011). Liberation technology: China's "Networked Authoritarianism". *Journal of Democracy*, *22*(2), 32–46.
Masnick, M. (2019). Protocols, not platforms: A technological approach to free speech. Knight First Amendment Institute at Columbia University, August 21. https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech
Mauldin, A. (2017). A complete list of content providers' submarine cable holdings. *TeleGeography*, November 9. https://blog.telegeography.com/telegeographys-content-providers-submarine-cable-holdings-list
Mazzucato, M. (2013). *The entrepreneurial state*. Anthem Press.
McChesney, R. W. (2013). *Digital disconnect: How capitalism is turning the internet against democracy*. The New Press.
Mueller, M. (2017). *Will the internet fragment?: Sovereignty, globalization and cyberspace*. Polity.
Mueller, M., & Kane, J. (2018). U.S. government should not reverse course on internet governance transition. *Brookings*, February 7. https://www.brookings.edu/blog/techtank/2018/02/07/u-s-government-should-not-reverse-course-on-internet-governance-transition/
Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance in international relations. *International Studies Review*, *15*(1), 86–104.
Musiani, F., & Pohle, J. (2014). NETmundial: Only a landmark event if "Digital Cold War" rhetoric abandoned. *Internet Policy Review*, *3*(1), 1–9.
Ni Loideain, N. (2015). EU law and mass internet metadata surveillance in the post-Snowden era. *Media and Communication*, *3*(2), 53–62.
Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111–130.
Pétin, P., & Tréguer, F. (2018). Building and defending the alternative internet: The birth of the digital rights movement in France. *Internet Histories*, *2*(3–4), 281–298.
Pohle, J. (2020). Digitale Souveränität. In T. Klenk, F. Nullmeier, & G. Wewer. (Eds.), *Handbuch Digitalisierung in Staat und Verwaltung* (pp. 1–13). Springer Fachmedien.
Pohle, J., & Thiel, T. (2019). Digitale Vernetzung und Souveränität: Genealogie eines Spannungsverhältnisses. In I. Borucki, & W. J. Schünemann (Eds.), *Internet und Staat: Perspektiven auf eine komplizierte Beziehung* (pp. 57–80). Nomos.
Radu, R. (2019). *Negotiating internet governance*. Oxford University Press.
Rühlig, T. N. (2020). *Technical standardisation, China and the future international order. A European perspective*. E-paper, Heinrich-Böll-Stiftung.
Schulze, M., & Voelsen, D. (2020). 'Einflusssphären Der Digitalisierung'. In B. Lippert, & S. Perthe (Eds.), *Strategische Rivalität Zwischen USA Und China: Worum Es Geht, Was Es Für Europa (Und Andere) Bedeutet* (pp. (32–36). Stiftung Wissenschaft und Politik. Deutsches Institut für Internationale Politik und Sicherheit.
Seoane, M. (2019). Alibaba's discourse for the digital silk road: The electronic world trade platform and "inclusive globalization". *Chinese Journal of Communication*, *13*(1), 1–16.
Shahbaz, A., & Funk, A. (2021). *Freedom on the net 2020. The pandemic's digital shadow, fueling digital repression worldwide*. Report, Freedom House.
Soldatov, A. (2019). Why Russia might shut off the internet. The Kremlin's Long obsession with central control. *Foreign Affairs*, March 29. https://www.foreignaffairs.com/articles/russian-federation/2019-03-29/why-russia-might-shut-internet
Steiger, S., Schünemann, W. J., & Dimmroth, K. (2017). Outrage without consequences? Post-Snowden discourses and governmental practice in Germany. *Media and Communication*, *5*(1), 7–16.
Stocker, V., Knieps, G., & Dietzel, C. (2021). The rise and evolution of clouds and private networks—Internet interconnection, ecosystem fragmentation. SSRN Scholarly Paper (ID 3910108).
ten Oever, N. (2021). "This is not how we imagined it": Technological affordances, economic drivers, and the internet architecture imaginary. *New Media & Society*, *23*(2), 344–362.
Tréguer, F. (2017). Intelligence reform and the Snowden paradox: The case of France. *Media and Communication*, *5*(1), 17–28.
Tréguer, F. (2019). *L'utopie Déchue*. Fayard.
Weinberg, J. (2011). Governments, privatization, and privatization: ICANN and the GAC. *Michigan Telecommunications and Technology Law Review*, *18*(1), 189–218.
Williams, J. (2018). *Stand out of our light: Freedom and resistance in the attention economy*. Cambridge University Press.
Winseck, D. (2017). The geopolitical economy of the global internet infrastructure. *Journal of Information Policy*, *7*, 228–267.

Zajacz, R. (2019). *Reluctant power: Networks, corporations, and the struggle for global governance in the early 20th century*. MIT Press.

Zuboff, S. (2018). *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. PublicAffairs.

How to cite this article: Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy & Internet*, 14, 13–27. https://doi.org/10.1002/poi3.296