Pohle, Julia; Thiel, Thorsten

Article

Digital sovereignty

Internet Policy Review

Provided in Cooperation with:
Alexander von Humboldt Institute for Internet and Society (HIIG), Berlin

Suggested Citation: Pohle, Julia; Thiel, Thorsten (2020) : Digital sovereignty, Internet Policy Review, ISSN 2197-6775, Alexander von Humboldt Institute for Internet and Society, Berlin, Vol. 9, Iss. 4, pp. 1-19,
https://doi.org/10.14763/2020.4.1532

This Version is available at:
https://hdl.handle.net/10419/233109

INTERNET POLICY REVIEW
Journal on internet regulation

Volume 9 | **Issue** 4

CONCEPT

OPEN ACCESS

PEER REVIEWED

Digital sovereignty

Julia Pohle *Berlin Social Science Center (WZB)*
Thorsten Thiel *Weizenbaum Institute* thorsten.thiel@wzb.eu

DOI: https://doi.org/10.14763/2020.4.1532

Published: 17 December 2020
Received: 11 July 2020 **Accepted:** 26 November 2020

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Keywords: Digital sovereignty, Internet governance, Internet exceptionalism, Digital economy, State authority

Abstract: Over the last decade, digital sovereignty has become a central element in policy discourses on digital issues. Although it has become popular in both centralised/authoritarian and democratic countries alike, the concept remains highly contested. After investigating the challenges to sovereignty apparently posed by the digital transformation, this essay retraces how sovereignty has re-emerged as a key category with regard to the digital. By systematising the various normative claims to digital sovereignty, it then goes on to show how, today, the concept is understood more as a discursive practice in politics and policy than as a legal or organisational concept.

This article belongs to **Concepts of the digital society**, a special section of *Internet Policy Review* guest-edited by Christian Katzenbach and Thomas Christian Bächle.

In July 2020, the German government, in its official programme for its presidency of the European Council, announced its intention "to establish digital sovereignty as a leitmotiv of European digital policy" (The German Presidency of the EU Council, 2020, p. 8). This is just one of the many recent episodes, albeit a very prominent one, in which the term *digital sovereignty* has been used by governments to convey the idea that states should reassert their authority over the internet and protect their citizens and businesses from the manifold challenges to self-determination in the digital sphere.

At first glance, the digital transformation and the global technical infrastructure of the internet seem to challenge sovereignty. The principles of territoriality and state hierarchy appear opposed to the diffuse, flexible, forever shifting constellations of global digital networks. What is more, digital applications and communication practices have created a momentum that seems to defy legal governance and control. Therefore, the growth of digital networks in the 1990s made the disappearance of the state an immediately plausible scenario. This was most famously captured in John Perry Barlow's bold *Declaration of the Independence of Cyberspace* (Barlow, 1996). Yet, while this reference is still very much alive in public discourse, today it is more often framed as a threat than a promise. To counter risks to their authority, states have made it possible to enforce national laws and undertake governmental interventions in the digital sphere. Over the years, they have created and reformed technical and legal instruments to address issues of digital governance (Goldsmith & Wu, 2006). In addition, they have successfully convinced their publics that sovereignty and state authority are necessary to protect "vital goods" ranging from security to prosperity, cultural rules and media control. As a result, in many countries, citizens today expect their governments to protect their privacy online or to combat online disinformation and cybercrime. But the various calls for digital sovereignty in the last few years, in both centralised/authoritarian countries and liberal democracies, do more than reaffirm state authority and intervention in the digital sphere. The concept of digital sovereignty has become a powerful term in political discourse that seeks to reinstate the nation state, including the national economy and the nation's citizens, as a relevant category in the global governance of digital infrastructures and the development of digital technologies. We can expect the concept of digital sovereignty to continue to gain even more political currency in the years to come, given the broad deployment of

highly invasive digital technologies ranging from artificial intelligence to the "Internet of Things".

To date, the concept of digital sovereignty has been widely used in political discourse but rarely scrutinised in academic research, with a small but growing number of exceptions (Couture & Toupin, 2019; Mueller, 2010, 2019; Pohle, 2020c; Pohle & Thiel, 2019; Thiel, 2014, 2019; Glasze & Dammann, in press; Peuker, 2020). To understand where the concept comes from and where it is headed, we proceed in two steps. First, we reconstruct key controversies that define the relationship between sovereignty and digital networks. We then analyse how the concept of sovereignty and statehood re-emerged and digital sovereignty was elevated to a cherished form of sovereignty in its own right. Secondly, we systematise the various claims to digital sovereignty, thereby highlighting the concept's internal tensions and contradictions. By tracing the dynamics of politicisation we attempt to show that sovereignty is a discursive practice in politics and policy rather than the legal and organisational concept that it is traditionally conceived of.

The relationship between sovereignty and the digital: a reconstruction

The political concept of sovereignty, understood as the power enjoyed by a governing body to rule over itself, free from any interference by outside sources or bodies, is derived from the Latin word *superanus*, which means "over" or "superior". Whereas the traditional theory of sovereignty, as proposed in the sixteenth century by French political philosopher Jean Bodin, concerned the ruler's authority to make final decisions, Jean-Jacques Rousseau recast the concept so that it focused on popular sovereignty rather than monarchical sovereignty; over time, it became increasingly associated with democracy, the rule of law and territoriality. Today, sovereignty always primarily means a state's independence *vis-à-vis* other states (external sovereignty) as well as its supreme power to command all powers within the territory of the state (internal sovereignty). Understood as democratic sovereignty, it encompasses popular sovereignty and citizens' right to exercise self-determination by making use of their inalienable rights. Crucial to all of these meanings is a geographical specification, that is, the restriction of sovereignty to a specific territory, which is seen as a functional prerequisite for authority to be exercised effectively (Grimm, 2015). [1]

1. Over the last decades, there have been many attempts to apply the concept of sovereignty to other political entities than states, such as supranational and sub-national institutions or indigenous peoples (e.g. Kukutai & Taylor, 2016). These derivative usages of the term often equalise sovereignty with autonomy and thereby deemphasise aspects of control and legitimation. While we believe

Ever since Bodin, sovereignty has been seen as a central concept for understanding politics. But in the 1990s, this importance seemed to wane, leading to talk of a post-sovereign world in which states would no longer be the most important and ultimately superior source of power and where democracy would be more closely associated with pluralism and participation than with the capacity of a demos to govern itself (MacCormick, 1999). This predicted decline in state importance strongly influenced the early stages of the internet's development and governance. The idea of state sovereignty was particularly challenged by two different, yet related, discursive strands that significantly shaped public and academic discourses: *cyber exceptionalism* and *multi-stakeholder internet governance*. Yet, in more recent years, policy actors have successfully sought to justify and reaffirm sovereignty in the digital sphere against these two perspectives.

Two challenges: cyber exceptionalism and internet governance

The first challenge, *cyber exceptionalism,* suggests that the digital realm is qualitatively distinctive from the analogue world and that digital spaces therefore need to be treated differently from all previous technological innovations. This perspective was especially popular during the rise of the commercial internet in the 1990s but is still evident in public and academic discourse. Cyber exceptionalist thinking is based on the assumption that the growing importance of computer-aided network communication implies the demise of state sovereignty (Katz, 1997). Although the internet's actual development did not take place outside of concrete legal spaces and would not have been possible without the incentives provided by markets, regulatory regimes or public research infrastructures (Mazzucato, 2011), cyber exceptionalism—which most often takes the form of *cyber libertarianism* (Keller, 2019)—was the formative ideology in those early days with a strong cultural and economic backing in Silicon Valley (Barbrook & Cameron, 1996; Turner, 2006).

As actors who greatly distrust established political institutions, cyber libertarians argue that digitally mediated forms of politics will prompt a decentralised organisation of societies. This should enable a better tailored response to the complex demands of governing modern societies than is offered by traditional forms of political organisation. In this view, external sovereignty, law and territoriality are expected to matter less in the context of transnational networks. The arguments for this are manifold. First, the complexity of nested responsibilities and the global

that these broader understandings are important and can partly explain the popularity of the concept of digital sovereignty, we stick to a more traditional political understanding of the term.

reach of networks cannot be addressed properly within national jurisdictions; second, legislative procedures are too slow to keep up with the pace of innovation of digital technologies and the associated business models; and third, digital technologies enable individuals to evade liability, because attribution becomes a shaky construct in the digital world (Post, 2007).Hence, in contrast to a world bound by territories and sovereign nations, the world invoked by cyber libertarianism requires the existence of *cyber sovereignty*, with *cyberspace* as a new and autonomous virtual realm that is independent of governmental interference (Barlow, 1996). [2]

The cyber exceptionalists and cyber libertarian positions still resonate today—for example, in the debates about cryptocurrencies (Pistor, 2020). But the main claim, namely that the rise of digital networks as such will lead to a demise of territorial conceptions of sovereignty, has lost its attraction. The infrastructures and the management of digital communication have steadily been transformed, making it easier to observe and steer digital flows. This trend has been reinforced by the commercialisation of the internet, as it has given rise to walled gardens and created new agents interested in a fine-grained, less anonymous and less horizontal architecture, which allows for intervention at many points (DeNardis, 2012; Deibert & Crete-Nishihata, 2012).

At least from the year 2000 onwards, a second, related but less confrontational challenge to sovereignty in its original sense emerged: *multi-stakeholder internet governance*. Here, the focus is not on states' shortcomings at regulating digital matters, but on the different and non-sovereign roles that states have to play in a regulatory ideal that views the administration of the internet as the task of those directly affected by it. Taking their origins in the technical community, characterised by expertise and meritocratic decision-making, a multiplicity of decentralised processes emerged, which were designed to serve the development and application of shared norms, rules and procedures to maintain and develop the internet (Klein, 2002; Chenou, 2014).In this vision, self-governance would take place in a multi-stakeholder governance structure based on the principles of openness, inclusion, bottom-up collaboration and consensual decision-making. This form of coordination, it was argued, could counteract the need for a central decision-making authority (Hofmann, 2016; Raymond & DeNardis, 2015).

2. A less pointed but still deeply state-sceptical variant of cyber exceptionalism is networked independence, a discursive stream frequently found in legal discourse and aligned with the discourse on globalisation and global governance. It argues that state sovereignty is in decline because of the dysfunctional fragmentation of a static order bound to geographical territories (Johnson & Post, 1996).

While multi-stakeholder internet governance has become established as a relatively autonomous field in the global policy arena, it is characterised by conflicts of various kinds. Its external conflicts are often rooted in the fact that the multi-stakeholder governance model continues to explicitly reject established government-dominated international institutions and seeks to replace them with the principle of transnationalism. Conversely, representatives of some states have insisted on putting the authority to make binding decisions on internet governance issues in the hands of multilateral institutions and, hence, subjecting them more heavily to state control (Musiani & Pohle, 2014; Glen, 2014). Internal conflicts in the field are caused by increasingly obvious coordination problems due to the multitude of often parallel internet governance processes as well as the thematic shift away from primarily technological matters towards more openly political or social questions (Malcolm, 2008). Furthermore, the idea of multi-stakeholder internet governance has often been accused of being associated with neoliberal thinking (Chenou, 2014). Thus, hopes of a lasting or expansive change in how transnational politics is done have not been fulfilled. Given the increasing attempts of both authoritarian and democratic nations to more strongly regionalise the development of digital networks, it is doubtful whether the efforts towards reforming multi-stakeholder internet governance will find the acceptance that would be necessary to preserve the model and its principles (Voelsen, 2019b).Therefore, multi-stakeholder internet governance cannot be seen as the future of governance as such, nor as a dichotomous alternative to decision-making by sovereign states, but rather as a parallel governance model adapted for non-binding coordination processes.

Resurgence of sovereignty as a principle of digital policy-making

In many respects, the public imaginary of digital communications as somehow hostile to state sovereignty and the practical challenges of enforcing sovereign power in the digital realm have remained (Mueller, 2010). But the arguments for dismissing state sovereignty have significantly weakened; instead, various actors have started to proclaim the need to establish sovereignty in the digital realm. The justifications for these calls are manifold.

First, it is often argued that the real challenge to state sovereignty is no longer to be found in the amorphous organisational qualities of decentralised networks, but in the enormous power of the corporate actors that thrive in our commercialised internet environment and that hold the material and immaterial power of owning vital societal structures. The internet's commercial focus has come to centre on advertising and the exploitation of network effects (Christl, 2017). Intermediaries and

digital platforms play such a dominant role in making content available that the open internet protocols that digital communications rely upon become meaningless (Pasquale, 2016; Srnicek, 2017; Hindman, 2018). Today, it is not just the enormous resources that those intermediaries command, but also the way in which they exercise control, that makes them one of the biggest challenges to the concept of democratic sovereignty (Staab, 2019; Zuboff, 2019). Internet corporations provide the infrastructures of our societies and, therefore, interfere with state matters at highly sensitive points. Examples abound: whether we are talking about the creation and regulation of markets or the provision and structuring of public communication, today's digital economy significantly differs from older constellations for ordering societies — to a point where many of the powerful corporate actors can be described as quasi-sovereign. The emergence of these corporate powerhouses, which appear to be largely unaccountable via traditional political mechanisms, has—especially in Europe—given rise to a new, more structural and often more expansive thinking about the demands and domains of democratic self-governance (van Dijck, 2020).

A second justification for enlarging and pushing digital sovereignty becomes most obvious when we look at the slightly paradoxical response of governments to Edward Snowden's 2013 revelations regarding the massive global surveillance practices of the United States' intelligence services and their allies (Tréguer, 2017, 2018; Steiger et al., 2017). Snowden revealed the mostly unconstrained exercise of hegemonic power and the enormous possibilities for data gathering, data analysis and data control by intelligence agencies and tech companies in the United States and other Western countries. Surprisingly, their decision to behave as sovereign yet non-territorial entities did not lead to a critique of power agglomeration as such (Hintz & Dencik, 2016). Instead, it triggered the demand for a decoupled digital sphere that allows for exclusive national control over communications, data and regulation. Ever since the Snowden revelations, demands for national (or regional) digital sovereignty are invoked by actors who highlight the risks of foreign surveillance and manipulation by citing examples ranging from disinformation (Tambiama, 2020) to telecommunication infrastructure (Voelsen, 2019a) and industrial policy (Hobbs et al., 2020).

If we sum up the observations made so far, we can see how (state) sovereignty, traditionally thought to be the bedrock of modern politics, has become a contested concept. Yet, it then slowly but forcefully found a way to accommodate itself in the digital age. Nowadays, justifications for insisting on sovereignty abound. Especially in international relations we can see a resurrection of sovereignty as a geopolitical

claim, which has set in motion a race to establish and expand the scope of sovereignty. Nevertheless, digital sovereignty needs to be actively explained and adjusted in order to fit our networked societies with their wide range of communications, strong transnational ties and pluralist understandings of democracy.

Political discourse(s) on digital sovereignty

Today, the concept of digital sovereignty is being deployed in a number of political and economic arenas, from more centralised and authoritarian countries to liberal democracies. It has acquired a large variety of connotations, variants and changing qualities. Its specific meaning varies according to the different national settings and actor arrangements but also depending on the kind of self-determination these actors emphasise (Pohle, 2020c; Lambach, 2019; Wittpahl, 2017). Focusing on this last factor, we can systematise digital sovereignty claims by distinguishing whether they address the capacity for digital self-determination by states, companies or individuals. What the different discursive layers resulting from this variety of claims share is their prescriptive and normative nature; rather than referring to existing instruments or specific practices, they usually formulate aspirations or recommendations for action. [3]

State autonomy and the security of national infrastructures

In the most prominent category of digital sovereignty claims, the emphasis is on the idea that a nation or region should be able to take autonomous actions and decisions regarding its digital infrastructures and technology deployment. The majority of these claims relate to the geographical restriction of sovereignty to a specific territory and to states' efforts ensuring the security of digital infrastructures and their authority regarding digital communication matters pertaining to their territories and citizens.

We can identify two strands of this line of thinking. On the one hand, powers outside of the liberal world have experienced the rise of networked communication as a threat to existing political systems. China was the first country to respond to this by propagating and developing its idea of digital sovereignty—mostly framed as *cyber sovereignty* or *internet sovereignty* (Creemers, 2016, 2020; Jiang, 2010; Zeng et al., 2017). The underlying ideas were later adapted by other authoritarian and se-

3. The proposed systematisation results from a structured qualitative analysis of selected policy documents applying the word digital sovereignty and similar terms (such as tech sovereignty, digital resilience, digital autonomy, etc.), which does not claim to be comprehensive. We use selected examples of policy texts and proposed measures to illustrate the different layers of digital sovereignty claims.

mi-authoritarian countries, most prominently Russia (Budnitsky & Jia, 2018; Stadnik, 2019; Nocetti, 2015). On the other hand, early on, Western states also addressed the need for control and independence in digital matters. Here the justification for creating architectures of control was mostly security-driven. As global networks emerged, states became more and more aware of their vulnerabilities, expressed in matters of infrastructural control. Computer security was then translated into national security and expanded to ever more areas (Nissenbaum, 2005; Hansen & Nissenbaum, 2009). In this process, the role and capacities of democractic states and of infrastructural control has grown strongly (Cavelty & Egloff, 2019)—although often times these practices have conflicted with liberal-democratic ideals of society and older understandings of technology as inclusive and pluralistic (Möllers, 2020). Since the 2013 Snowden revelations, the focus on state autonomy and security has become a core element of digital sovereignty discourses.

Prime examples of government-fostered practices and ideas resulting from this discursive strand are the many recent proposals towards data localisation. They seek to restrict the storage, movement and/or processing of data to specific areas and jurisdictions and are typically justified by the need to limit the access that foreign intelligence and commercial agencies may have to specific types of data, for example, industrial or personal data. It is often assumed, but rarely clearly stated, that many such proposals are also driven by other motivations, such as the increased accessibility of citizens' data by intelligence actors and law-enforcement agencies and the wish to generate revenues for actors like local internet service providers (Chander & Le, 2015; Hill, 2014). In many countries, including Brazil and India—two important emerging economies—proposals towards data localisation have so far only been realised in fragmented form or remain limited to specific contexts (Panday & Malcom, 2018; Selby, 2017). An emblematic case of a proposed data localisation initiative in Europe is the *Schengen Routing* idea, that is, the proposal to avoid routing data flows within Europe via exchange points and routes outside of Europe (Glasze & Dammann, in press, p. 11). The idea, which was proposed by Deutsche Telekom, the largest internet provider in Germany and the largest telecommunications organisation in the European Union, was hotly debated both in the public and the political sphere but ultimately failed to garner sufficient political support (Kleinhans, 2013).

Present in both authoritarian and democratic countries, claims and proposed measures emphasising the autonomy and self-determination of states and the security of critical digital infrastructures have been met with fierce criticism. Both policy actors and observers, such as academics and technical experts, fear that efforts fo-

cusing on IT security and the regulation of internet issues on the national level would interfere with the open and universally accessible nature of the internet (Maurer et al., 2014) and ultimately lead to the *re-territorialisation* of the global internet, causing its *fragmentation* into national internet segments (Drake et al., 2016; Mueller, 2017). This, in return, may have important negative economic and political impacts for the countries concerned due to their digital and geographical isolation (Hill, 2014).

Economic autonomy and competition

There is a second category of digital sovereignty claims, which is closely related, yet different from the focus on state autonomy. This emphasises the high and often opposing economic stakes surrounding the digital environment and focuses on the autonomy of the national economy in relation to foreign technology and service providers. Like the previous category of assertions, claims focusing on economic self-determination have been primarily spurred by the perceived market dominance of technology companies from the United States and increasingly also China (Steiger et al., 2017, p. 11). Likewise, the specific measures and instruments that governments apply to compensate for these imbalances in the digital economy partly overlap with measures seeking to strengthen the security of technological systems and national autonomy (Baums, 2016). But in contrast to the first category, these measures are usually part of a nation's larger economic and industrial policy strategy, aiming at the digital transformation of entire sectors of the economy. As such, they concern both traditional industries and sectors (telecommunications, media, logistics) and new IT-related economic sectors, and primarily aim to promote the innovative power of the domestic economy and to nurture local competitors (Bria, 2015). In addition, a growing number of instruments centre on digital trade and seek to regulate commerce and data flows delivered via digital networks (Burri, 2017; Ferracane, 2017).

A prime example of an initiative that seeks to strengthen economic autonomy is the European cloud service Gaia-X, which was announced jointly by France and Germany in 2019 and is yet to be launched (BMWi, 2020). The project plans to connect small and medium-sized cloud providers in Europe through a shared standard that allows them to offer an open, secure and trustworthy European alternative to the world's biggest (often US-based) cloud service providers (e.g., Amazon, Google, Microsoft), while at the same time respecting European values and data protection standards. The initiative is heavily promoted by policy actors as an important step towards European *data sovereignty* (BMBF, 2019a; Summa, 2020)—another closely related concept. But it has already been criticised for being an overly ambitious

and purely state-driven project that does not offer real innovation and that will have to compete for market acceptance with more established providers (Lumma, 2019; Mahn, 2020).

As with the previous category, the goal to achieve more independence from foreign technologies and to promote the innovative power of the domestic industry is a central element of discourses on digital sovereignty in both authoritarian and democratic countries. In democratic countries, some measures are additionally justified by the aim to protect consumers by offering technological services that respect user rights and domestic laws and norms such as data protection regulations (Hill, 2014; Mauer et al., 2014, p. 8). In many emerging economies, such as India, the proposed measures are also often clearly directed at what has been described by both policy actors and scholars as *digital imperialism* or *digital colonialism*. Both terms refer to the overly dominant position of Western technology corporations in the Global South which leads to new forms of hegemony and exploitation (Pinto, 2018; Kwet, 2019; PTI, 2019). Unsurprisingly, such claims and initiatives have been met with scepticism and repudiation by some Western countries, where policy and business actors have been quick to label such ideas and practices *digital protectionism*, meaning the "erection of barriers or impediments to digital trade" (Aaronson, 2016, p. 8; see also Aaronson & Leblond, 2018). But while in the United States, where the notion of digital sovereignty has principally a negative connotation (Couture & Toupin, 2019, p. 2313), a wide variety of policies are considered potentially protectionist—including censorship, filtering, localisation and intellectual property-related measures and regulations to prevent disinformation and to protect privacy—in other regions and countries, such as Europe and Canada, narrower definitions that account for specific trade restrictions due to privacy concerns and cultural exceptions have been proposed (Aaronson, 2016, p. 10).

User autonomy and individual self-determination

In recent years, a third category of digital sovereignty claims has emerged. This is primarily present in the discourses of democratic countries and a particularly strong component of the policy debate on digital sovereignty in Germany (Pohle, 2020a, p. 7ff.; Glasze & Dammann, in press, p. 13). Emphasising the importance of individual self-determination, these claims focus on the autonomy of citizens in their roles as employees, consumers, and users of digital technologies and services. An interesting aspect of this category is the departure from a state-centred understanding of sovereignty. Instead of viewing sovereignty as the prerequisite to exercise authority in a specific territory, actors view it as the ability of individuals to take actions and decisions in a conscious, deliberate and independent manner.

By strengthening these capacities, individuals should be protected as consumers and strengthened in their rights as democratic citizens (Gesellschaft für Informatik, 2020; VZBV, 2014). Discursive claims by policy makers and civil society actors in this category also refer to user sovereignty and digital consumer sovereignty, thereby replacing the control of users and citizens who might be subject to digital sovereignty measures in authoritarian regimes with the goal to strengthen domestic internet users' capacity for self-determination (Pohle, 2020c, p. 8ff.; SVRV, 2017).

The proposed means to achieve this kind of sovereignty in the digital sphere include economic incentives for user-friendly and domestic technology development, but also the introduction of technical features allowing for effective encryption, data protection and more transparent business models. In addition, a large majority of measures targeting individual self-determination seek to enhance users' media and digital literacy, thus strengthening the competences and confidence of users and consumers in the digital sphere. In Germany, for example, a recently created innovation fund by the Federal Ministry of Education and Research (the "Human-Technology-Interaction for Digital Sovereignty" fund) builds on the idea that digital literacy means more than being technologically knowledgeable or competent in the use of digital tools. Rather, it is understood as the critical or conscious engagement of users with the technology and their own data (*Datenbewusstsein*, see BMBF, 2019b).

An interesting aspect of this discursive category of digital sovereignty is the references made to users' technological or digital sovereignty made by tech activists and social movements. Their perspective contradicts a state-centred understanding of sovereignty and instead emphasises the need for users to better understand commercial and state powers in the digital sphere and to appropriate their technologies, data and content (Couture & Toupin, 2019, p. 2315ff). This could either be done by prioritising open and free software and service or by users protecting themselves from the exploitation of their personal data by tech companies through data protection and encryption practices (Haché, 2014, 2018; Cercy & Nitot, 2016). While some facets of this perspective and some of the proposed measures may align with the claims to individual self-determination that we can see in democracies, the underlying beliefs are, however, different. Moreover, references made and measures suggested by policymakers seeking to increase user sovereignty need to be evaluated very carefully. In many instances, citizens are being reduced to consumers of digital services rather than valued in their capacity as democratic citizens. But the focus on the autonomy and security of consumers might

obfuscate measures that primarily serve security and economic purposes, leading to a situation in which fundamental user rights—such as privacy or freedom of expression—are restricted rather than enforced.

Sovereignty in the networked world

This essay has argued that advocates of the concept of digital sovereignty, so popular in political and public discourse nowadays, not only had to reverse some of their early beliefs about the governability of a networked world but that the idea of sovereignty itself has shifted as it has risen to prominence. The issue is no longer *cyber sovereignty* as a non-territorial challenge to sovereignty that is specific to the virtual realm of the internet. Today, *digital sovereignty* has become a much more encompassing concept, addressing not only issues of internet communication and connection but also the much wider digital transformation of societies. Digital sovereignty is—especially in Europe—now often used as a shorthand for an ordered, value-driven, regulated and therefore reasonable and secure digital sphere. It is presumed to resolve the multifaceted problems of individual rights and freedoms, collective and infrastructural security, political and legal enforceability and fair economic competition (Bendiek & Neyer, 2020).

Traditionally, sovereignty has largely been thought of as an enforceable law that is backed by clear structural arrangements, such as the state monopoly on violence. In this context, the state is conceived of as a more or less coherent actor, capable, independent and hence autonomous. Although sovereignty has always been imperfect—Stephen Krasner famously depicted it as "organized hypocrisy" (Krasner, 1999)—the means of sovereign power in the Westphalian system have been rather straightforward. But due to digitalisation, globalisation and platformisation the situation has become more complicated. The digital sovereignty of a state cannot be reduced to its ability to set, communicate and enforce laws. Rather than relying on the symbolic representation and organisational capacity of the state, digital sovereignty is deeply invasive. In many instances, the idea of strengthening digital sovereignty means not only actively managing dependencies, but also creating infrastructures of control and (possible) manipulation. Therefore, we believe that much more reflection and debate is needed on how sovereign powers can be held democratically accountable with regard to the digital. It is not sufficient to propose that the power of large digital corporations could be tamed by subjecting them to democratic sovereignty, as has been suggested by many democratic governments worldwide. Likewise, we should not simply equate (digital) sovereignty with the ability to defend liberal and democratic values, as is often done by policy actors in

Europe. Digital sovereignty is not an end in itself. Instead, we have to put even more thought into the procedural framework of how sovereign power can be held accountable and opened up to public reflection and control in order to truly democratise digital sovereignty.

References

Aaronson, S. A. (2016). *The digital trade imbalance and its implications for internet governance* (Paper No. 25; Global Commission on Internet Governance). Centre for International Governance Innovation.

Aaronson, S. A., & Leblond, P. (2018). Another digital divide: The rise of data realms and its implications for the WTO. *Journal of International Economic Law*, *21*(2), 245–272. https://doi.org/10.1093/jiel/jgy019

Barbrook, R., & Cameron, A. (1996). The Californian ideology. *Science as Culture*, *6*(1), 44–72. https://doi.org/10.1080/09505439609526455

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace*. *Electronic Frontier Foundation*. https://www.eff.org/cyberspace-independence

Baums, A. (2016). Digitale Standortpolitik in der Post-Snowden-Welt. In M. Friedrichsen & P.-J. Bisa (Eds.), *Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft* (pp. 223–235). Springer VS. https://doi.org/10.1007/978-3-658-07349-7_20

Bendiek, A., & Neyer, J. (2020). Europas digitale Souveränität. Bedingungen und Herausforderungen internationaler politischer Handlungsfähigkeit. In M. Oswald & I. Borucki (Eds.), *Demokratietheorie im Zeitalter der Frühdigitalisierung* (pp. 103–125). Springer VS.

B.M.B.F. (2019a). *"GAIA-X": Ein neuer Datenraum für Europa*. Bundesministerium für Bildung und Forschung. https://www.bmbf.de/de/gaia-x-ein-neuer-datenraum-fuer-europa-9996.html

B.M.B.F. (2019b). *Mensch-Technik-Interaktion für digitale Souveränität—Mensch-Technik-Interaktion*. Bundesministerium für Bildung und Forschung. https://www.technik-zum-menschen-bringen.de/foerderung/bekanntmachungen/digisou

BMWi. (2020). *GAIA-X: A Federated Data Infrastructure for Europe*. Bundesministerium für Wirtschaft und Energie. https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html

Bria, F. (2015). *Public policies for digital sovereignty*. Platform Cooperativism Consortium conference, New York. https://www.academia.edu/19102224/Public_policies_for_digital_sovereignty

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies*, *21*(5), 594–613. https://doi.org/10.1177/1367549417751151

Burri, M. (2017). The Regulation of Data Flows through Trade Agreements. *Georgetown Journal of International Law*, *48*(1), 408–448.

Cavelty, M. D., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, *15*(1), 37–57. https://www.ingentaconnect.com/content/stair/

stair/2019/00000015/00000001/art00004

Cercy, N., & Nitot, T. (2016). *Numérique: Reprendre le contrôle*. Framasoft.

Chander, A., & Le, U. P. (2015). Data Nationalism. *Emory Law Journal*, *64*(6), 677–739.

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. https://doi.org/10.1080/14747731.2014.887387

Christl, W. (2017). *Corporate Surveillance In Everyday Life. How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions* [Report]. Cracked Labs. http://crackedlabs.org/en/corporate-surveillance

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(2), 2305–2322. https://doi.org/10.1177/1461444819865984

Creemers, R. (2016). *The Chinese cyber-sovereignty agenda* (M. Leonard, Ed.). European Council on Foreign Relations.

Creemers, R. (2020). China's Conception of Cyber Sovereignty. In D. Broeders & B. Berg (Eds.), *Governing Cyberspace: Behavior, Power and Diplomacy* (pp. 107–145). Rowman & Littlefield.

Deibert, R. J., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance*, *18*(3), 339–361. https://doi.org/10.1163/19426720-01803006

DeNardis, L. (2012). Hidden Levers of Internet Control. *Information, Communication & Society*, *15*(5), 720–738. https://doi.org/10.1080/1369118X.2012.659199

Drake, W. J., Cerf, V. G., & Kleinwächter, W. (2016). *Internet Fragmentation: An Overview* (Future of the Internet Initiative) [White Paper]. World Economic Forum. https://www.weforum.org/reports/internet-fragmentation-an-overview.

Ferracane, M. (2017). *Restrictions on Cross-Border Data Flows: A Taxonomy* (Working Paper No. 1/2017). European Centre for International Political Economy. https://doi.org/10.2139/ssrn.3089956

Gesellschaft für Informatik. (2020). *Schlüsselaspekte Digitaler Souveränität* [Working Paper]. Gesellschaft für Informatik. https://gi.de/fileadmin/GI/Allgemein/PDF/Arbeitspapier_Digitale_Souveraenitaet.pdf

Glasze, G., & Dammann, F. (in press). Von der „globalen Informationsgesellschaft" zum „Schengenraum für Daten" – Raumkonzepte in der Regierung der „digitalen Transformation" in Deutschland. In T. Döbler, C. Pentzold, & C. Katzenbach (Eds.), *Räume digitaler Kommunikation (forthcoming*. Halem.

Glen, C. M. (2014). Internet Governance: Territorializing Cyberspace? *Politics & Policy*, *5*(42), 635–657. https://doi.org/10.1111/polp.12093

Goldsmith, J., & Wu, T. (2006). *Who controls the internet? Illusions of a borderless world*. Oxford University Press.

Grimm, D. (2015). *Sovereignty: The Origin and Future of a Political and Legal Concept*. Columbia University Press.

Haché, A. (2014). *La Souveraineté technologique* (Vol. 1). Dossier ritimo. https://www.ritimo.org/La-Souverainete-technologique.

Haché, A. (2018). *La Souveraineté technologique—Volume 2. Dossier ritimo*. https://www.ritimo.org/La-Souverainete-Technologique-Volume2.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hill, J. F. (2014). The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. *Policymakers and Industry Leaders. Lawfare Research Paper Series*, *2*(3), 1–41.

Hindman, M. (2018). *The Internet trap: How the digital economy builds monopolies and undermines democracy*. Princeton University Press. https://doi.org/10.23943/princeton/9780691159263.001.0001

Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, *5*(3). https://doi.org/10.14763/2016.3.424

Hobbs, C. (Ed.). (2020). *Europe's digital sovereignty: From rulemaker to superpower in the age of US-China rivalry*. European Council on Foreign Relations. https://ecfr.eu/publication/europe_digital_sovereignty_rulemaker_superpower_age_us_china_rivalry/.

Hofmann, J. (2016). Multi-stakeholderism in Internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, *1*(1), 29–49. https://doi.org/10.1080/23738871.2016.1158303

Jiang, M. (2010). Authoritarian Informationalism: China's Approach to Internet Sovereignty. *SAIS Review of International Affairs*, *30*(3), 71–89. https://doi.org/10.1353/sais.2010.0006

Johnson, D. R., & Post, D. G. (1996). Law and Borders—The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/10.2307/1229390

Katz, J. (1997). Birth of a Digital Nation. In *Wired*. https://www.wired.com/1997/04/netizen-3/.

Keller, C. I. (2019). *Exception and Harmonization: Three Theoretical Debates on Internet Regulation* (2020(2); HIIG Discussion Paper Series). Alexander von Humboldt Institut für Internet und Gesellschaft. https://doi.org/10.2139/ssrn.3572763

Klein, H. (2002). ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy. *The Information Society*, *18*(3), 193–207. https://doi.org/10.1080/01972240290074959

Kleinhans, J.-P. (2013, November 13). Schengen-Routing, DE-CIX und die Bedenken der Balkanisierung des Internets. *Netzpolitik*. https://netzpolitik.org/2013/schengen-routing-de-cix-und-die-bedenken-der-balkanisierung-des-internets/.

Krasner, S. D. (1999). *Sovereignty: Organized Hypocrisy*. Princeton. https://doi.org/10.2307/j.ctt7s9d5

Kukutai, T., & Taylor, J. (2016). *Indigenous data sovereignty: Toward an agenda*. Anu Press.

Kwet, M. (2019). Digital colonialism: US empire and the new imperialism in the Global South. *Race & Class*, *60*(4), 3–26. https://doi.org/10.1177/0306396818823172

Lambach, D. (2019). The Territorialization of Cyberspace. *International Studies Review*, *22*(3), 482–506. https://doi.org/10.1093/isr/viz022

Lumma, N. (2019). Die „europäische Cloud" ist eine Kopfgeburt, die nicht überleben wird. *Gründerszene Magazin*. https://www.gruenderszene.de/technologie/gaia-x-europaeische-cloud-wird-scheitern

MacCormick, N. (1999). *Questioning Sovereignty: Law, State, and Nation in the European Commonwealth*. Oxford University Press.

Mahn, J. (2020). Die digitale europäische Idee. Gaia-X: Wie Europa in der Cloud unabhängig werden soll. *Magazin für Computertechnik*, *14*. https://www.heise.de/select/ct/2020/14/2015610312088025860

Malcolm, J. (2008). *Multi-stakeholder governance and the Internet Governance Forum*. Terminus Press.

Maurer, T., Morgus, R., Skierka, I., & Hohmann, M. (2014). *Technological Sovereignty: Missing the Point?* [Paper]. New America; Global Public Policy Institute. http://www.digitaldebates.org/fileadmin/media/cyber/Maurer-et-al_2014_Tech-Sovereignty-Europe.pdf

Mazzucato, M. (2011). *The entrepreneurial state*. Demos. http://oro.open.ac.uk/30159/1/Entrepreneurial_State_-_web.pdf

Möllers, N. (2020). Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State. *Science, Technology, & Human Values*, *46*(1), 112–138. https://doi.org/10.1177/0162243920904436

Mueller, M. (2017). *Will the internet fragment?: Sovereignty, globalization and cyberspace*. Polity.

Mueller, M. (2020). Against Sovereignty in Cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Mueller, M. L. (2010). *Networks and States: The Global Politics of Internet Governance*. MIT Press. https://doi.org/10.7551/mitpress/9780262014595.001.0001

Musiani, F., & Pohle, J. (2014). NETmundial: Only a Landmark Event If "Digital Cold War" Rhetoric Abandoned. *Internet Policy Review*, *3*(1). https://doi.org/10.14763/2014.1.251

Nissenbaum, H. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology*, *7*(2), 61–73. https://doi.org/10.1007/s10676-005-4582-3

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111–130. https://doi.org/10.1111/1468-2346.12189

Panday, J., & Malcolm, J. (2018). The Political Economy of Data Localization. *Partecipazione e conflitto*, *11*(2), 511–527. https://doi.org/10.1285/i20356609v11i2p511

Pasquale, F. (2016). Two narratives of platform capitalism. *Yale Law & Policy Review*, *35*(1), 309–321. https://ylpr.yale.edu/two-narratives-platform-capitalism

Peuker, E. (2020). *Verfassungswandel durch Digitalisierung*. Mohr Siebeck.

Pinto, R. Á. (2018). Digital Sovereignty or Digital Colonialism? New tensions of privacy, security and national policies. *Sur*, *15*(27), 15–27. https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/

Pistor, K. (2020). Statehood in the digital age. *Constellations*, *27*(1), 3–18. https://doi.org/10.1111/1467-8675.12475

Pohle, J. (2020a). Digitale Souveränität. In T. Klenk, F. Nullmeier, & G. Wewer (Eds.), *Handbuch Digitalisierung in Staat und Verwaltung* (pp. 1–13). Springer. https://doi.org/10.1007/978-3-658-23669-4_21-1

Pohle, J. (2020b). *Digital sovereignty – a new key concept of digital policy in Germany and Europe*

[Research paper]. Konrad Adenauer Stiftung. https://www.kas.de/en/single-title/-/content/digital-sovereignty

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.

Post, D. G. (2007). Governing Cyberspace: Law. *Santa Clara High Technology Law Journal*, *24*(4), 883–913. https://digitalcommons.law.scu.edu/chtlj/vol24/iss4/5/

P.T.I. (2019, January 20). India's data must be controlled by Indians: Mukesh Ambani. *mint*. https://www.livemint.com/Companies/QMZDxbCufK3O2dJE4xccyI/Indias-data-must-be-controlled-by-Indians-not-by-global-co.html

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616. https://doi.org/10.1017/S1752971915000081

Selby, J. (2017). Data localization laws: Trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology*, *25*(3), 213–232. https://doi.org/10.1093/ijlit/eax010

Srnicek, N. (2017). The challenges of platform capitalism. Understanding the logic of a new business model. *Juncture*, *23*(4), 254–257. https://doi.org/10.1111/newe.12023

Staab, P. (2019). *Digitaler Kapitalismus: Markt und Herrschaft in der Ökonomie der Unknappheit*. Suhrkamp.

Stadnik, I. (2019). *Internet Governance in Russia–Sovereign Basics for Independent Runet*. 47th Research Conference on Communication, Information and Internet Policy (TPRC47). https://doi.org/10.2139/ssrn.3421984

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. https://doi.org/10.17645/mac.v5i1.814

Summa, H. A. (2020, March). How GAIA-X is Paving the Way to European Data Sovereignty. *Dotmagazine*. https://www.dotmagazine.online/issues/cloud-and-orientation/build-your-own-internet-gaia-x

SVRV (Advisory Council for Consumer Affairs). (2017). *Digitale Sourveränität*. Sachverständigenrat für Verbraucherfragen.

Tambiama, M. (2020). *Digital sovereignty for Europe* (EPRS Ideas Papers, pp. 1–12) [Briefing]. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

The German Presidency of the EU Council. (2020). *Together for Europe's recovery: Programme for Germany's Presidency of the Council of the European Union (1 July to 31 December 2020)*. Council of the European Union.

Thiel, T. (2014). Internet und Souveränität. In C. Volk & F. Kuntz (Eds.), *Der Begriff der Souveränität in der transnationalen Konstellation* (pp. 215–239). Nomos.

Thiel, T. (2019). Souveränität: Dynamisierung und Kontestation in der digitalen Konstellation. In J. Hofmann, N. Kersting, C. Ritzi, & W. J. Schünemann (Eds.), *Politik in der digitalen Gesellschaft: Zentrale Problemfelder und Forschungsperspektiven* (pp. 47–61). Transcript.

Tréguer, F. (2017). Intelligence reform and the Snowden paradox: The case of France. *Media and Communication*, *5*(1), 17–28. https://doi.org/10.17645/mac.v5i1.821

Tréguer, F. (2018). *US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance*. (Research Report No. 5; UTIC Deliverables). SciencesPo. https://halshs.archives-ouvertes.fr/halshs-01865140

Turner, F. (2006). *From counterculture to cyberculture: Stewart Brand, the Whole Earth Network, and the rise of digital utopianism*. University of Chicago Press.

van Dijck, J. (2020). Governing digital societies: Private platforms, public values. *Computer Law & Security Review*, *36*. https://doi.org/10.1016/j.clsr.2019.105377

Voelsen, D. (2019a). *5G, Huawei und die Sicherheit unserer Kommunikationsnetze – Handlungsoptionen für die deutsche Politik* (Report No. 5; SWP-Aktuell). Stiftung Wissenschaft und Politik. German Institute for International and Security Affairs. https://doi.org/10.18449/2019A05

Voelsen, D. (2019b). *Cracks in the internet's foundation: The future of the internet's infrastructure and global internet governance* (Research Paper No. 14). Stiftung Wissenschaft und Politik. German Institute for International and Security Affairs. https://doi.org/10.18449/2019RP14

VZBV (Federation of German Consumer Organisations). (2014). *Digitalisierung: Neue Herausforderungen für Politik und Verbraucher* [Press release]. https://www.vzbv.de/pressemitteilung/digitalisierung-neue-herausforderungen-fuer-politik-und-verbraucher

Wittpahl, V. (Ed.). (2017). *Digitale Souveränität: Bürger, Unternehmen, Staat*. Springer Vieweg. https://doi.org/10.1007/978-3-662-55796-9

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty". *Politics & Policy*, *45*(3), 432–464. https://doi.org/10.1111/polp.12202

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Published by

Alexander von Humboldt Institute for Internet and Society

in cooperation with

CREATe

centre internet et société

R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya