Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices

Francesca Musiani

▶ To cite this version:

Francesca Musiani. Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. Information, Communication and Society, 2022, Special Issue AoIR 2021, "Independence", pp.1-16. 10.1080/1369118X.2022.2049850 . hal-03607812

HAL Id: hal-03607812
https://hal.science/hal-03607812

Submitted on 14 Mar 2022

Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-Based Sociology of Digital Self-Determination Practices

Francesca Musiani

Centre for Internet and Society, CNRS, Paris, France

CIS, 59-61 rue Pouchet, 75017 Paris, France. E-mail : francesca.musiani@cnrs.fr

Associate Research Professor, CNRS and Deputy Director, CIS

https://cis.cnrs.fr/francesca-musiani/

@franmusiani

Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-Based Sociology of Digital Self-Determination Practices

Today, a number of high-profile initiatives across the globe are concrete implementations of the "digital sovereignty" principle: i.e. the idea that states should "reaffirm" their authority over the Internet and the broader digital ecosystem, to protect their citizens, institutions, and businesses from the multiple challenges to their nation's self-determination in the digital sphere. According to this principle, sovereignty depends on more than supranational alliances or international legal instruments, military might or trade: it depends on locally-owned, controlled and operated innovation ecosystems, able to increase states' technical and economic independence and autonomy. Presently, digital sovereignty is understood primarily as a legal concept and a set of political discourses. As a consequence, it is predominantly analysed by political science, international relations and international law. However, the study of digital sovereignty as a set of infrastructures and socio-material practices has been comparatively neglected. This article explores how the concept of digital sovereignty can be studied via the infrastructure-embedded "situated practices" of various political and economic projects which aim to establish autonomous digital infrastructures in a hyperconnected world. Although the article focuses primarily on outlining the agenda for a wider and comparative research programme, I will place a specific focus on Russia, subject of an ongoing research project, as a pilot case.

Keywords: digital sovereignty; digital infrastructures; Internet infrastructures; situated practices; digital autonomy: digital self-determination; infrastructuring

Introduction

In June 2020, under the impulse of a Franco-German effort launched in 2019, ministers from France and Germany met to formally launch GAIA-X, the "next-generation secure data infrastructure" for the European Union[1]. With the explicit objective of enhancing Europe's "independence" from cloud computing giants in both the United States and China, GAIA-X is meant to boost Europe's own digital ecosystem under the umbrella of the most recent European data protection legislation; an ambitious goal, with politico-technical controversies in its wake, such as American big data analytics firm Palantir joining the project in December 2020 (a decision validated by GAIA-X's Board of Directors in February 2021)[2]. This case, and manifold others in recent history, shows how digital infrastructures – shorthand for advanced digital technologies[3], networks and services, the Internet first and foremost, which facilitate communication and the creation, storage, analysis and sharing of data and information – materialize broader transformations in which sovereignty, territories, national and supra-national institutions are co-produced. Never in history has it been clearer than today: digital infrastructures, from the physical ones (submarine cables, data centers, Internet Exchange Points) to the "logical" ones (protocols such as IP or algorithms such as Google's PageRank) are crucial components in arrangements of power.

"Digital sovereignty", "technological sovereignty", "Internet sovereignty" – especially since the former NSA contractor Edward Snowden disclosed the pervasive practice of digital surveillance, these different terms have increasingly been put forward to convey the idea that states should "reaffirm" their authority over the Internet and

[1] https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html

[2] https://blog.cryptshare.com/en/gaia-x-board-of-directors-gives-green-light-to-palantir

[3] Which is admittedly, to some extent, shorthand itself.

protect their citizens, institutions, and businesses from the multiple challenges to their nation’s self-determination in today’s digital sphere. According to this principle, sovereignty depends on more than supranational alliances or international legal instruments, military might or trade: it depends on locally-owned, controlled and operated innovation ecosystems, able to increase states’ technical and economic independence and autonomy.

Presently, digital sovereignty is understood primarily as a legal concept and a set of political discourses. As a consequence, it is predominantly analysed by political science, international relations and international law. However, the study of digital sovereignty as a set of infrastructures and socio-material practices has been, so far, largely neglected. This article’s primary aim is to outline a research agenda aimed at filling this gap. We suggest that, as the “digital sovereignty” label is increasingly mobilized by both practitioners and scholars of Internet and digital governance, a perspective grounded in science and technology studies (STS) and more specifically in infrastructure studies is a useful and yet-underdeveloped theoretical and methodological innovation that allows to examine the co-development of material, institutional, and territorial components of digital sovereignty. The digital in “digital sovereignty” is ultimately a matter of situated and embedded materials that are of interest to politics and its scholars, and that specialists of technology and its sociology can contribute to untangle.

Internet infrastructures have long been recognized, especially in the STS tradition, as crucial sites in which power relations materialize. This article makes a case for infrastructures as theoretically and methodologically important for making sense of “digital sovereignty”. The key is to look at what infrastructures and related practices actually *do* and shape, rather than treating them, as literature on digital governance has often done, as *external* causes of the erosion of state power and territory. Such a perspective allows to shed new light on how strategies of digital sovereignty get inscribed in infrastructures, and understand what this reveals of transformations in institutions and territories, thereby deconstructing and reconstructing the concept of digital sovereignty by examining its concrete embodiments in technical infrastructures. This article explores how the concept of digital sovereignty can be studied via the infrastructure-embedded "situated practices" of various political and economic projects which aim to establish autonomous digital infrastructures in a hyperconnected world. Although the article focuses primarily on outlining the agenda for a wider and comparative research program, centered on the notion I call "infrastructuring digital sovereignty", the last part of the article will place a specific focus on Russia, subject of an ongoing research project, as a pilot case and current testbed for this analytical framework.

Framing the infrastructures (and the *infrastructuring*) of digital sovereignty

The research agenda proposed in this article seeks to interweave three lineages of literature. The first lineage includes literature in Internet governance (IG) studies and in particular its subset that addresses the concept of digital sovereignty and the relationship between digital networks and states, including work on the re-territorialisation and fragmentation of the global Internet, on past and present imaginaries of digital governance and on the relationship between statehood, territories, and digital networks. The second lineage encompasses studies of information systems according to perspectives in STS and more specifically in infrastructure studies, which have sought to understand where conflicts and controversies emerge and how they take shape with infrastructures, as well as arrangements of power inherent in technical infrastructures and architectures of digital technologies, and revealed by them. The third, more recent, lineage focuses on the notion of the “turn to infrastructure” in Internet governance (Musiani et al., 2016) as a key to examine the cooptation of digital infrastructures for political objectives.

Internet governance studies of digital sovereignty and state transformations

From a multidisciplinary perspective, Internet governance (IG) can be understood as a set of sociotechnical and political processes of innovation, digitalisation, regulation, mobilisation, co-optation, ordering and reflexive coordination concerning the infrastructure of the Internet, its applications and usages (DeNardis, 2014; Hofmann et al., 2017). Analytical reflections and normative claims about the role played by states and governments in the governance structures of the Internet have always been central for the community of scholars interested in IG. Since the earliest research on the societal and political effects of digital networks in the 1990s, scholars have tried to understand the effect that the Internet as a digital, transnational and decentralised networking technology would have on the importance of territory, borders and states. Initially, many observers expected digital networks to increase the effect of globalisation, leading to a general decline in the importance of the nation state (Elden, 2005). Proponents of so-called *cyber exceptionalism,* in particular, viewed the Internet as a new kind of virtual space which was independent from geographical space and, therefore, irreconcilable with the idea of nation-state-based and territorial sovereignty (Johnson & Post, 1996).

Although this perspective continues to be influential in IG research, scholars oppose it by arguing that states can and do influence and control the development and use of digital networks through legislation and regulation (e.g. Goldsmith & Wu, 2006) or by setting technical standards (e.g. Lessig, 1999; Deibert & Crete-Nishihata 2012). Acknowledging that the global infrastructure of the Internet needs some form of global coordination in order to function and grow, these scholars often focus on the role of governments and intergovernmental organisations in the global governance system of the Internet. Accordingly, they analyse the emergence of an institutional framework for IG and the role played by states in the creation and working of institutions like ICANN (e.g. Klein, 2002) or for policy debates at global events such as the World Summit on the Information Society (e.g. Raboy et al., 2010) or the Internet Governance Forum (e.g. Malcolm, 2008). While many scholars seek to assess the contributions made by state actors to multi-stakeholder governance arrangements (e.g. Hofmann, 2016), other authors focus on the conflicts emerging in global IG between different governments or between states and other stakeholder groups (e.g. Mueller, 2010).

Shifting the focus from the global coordination of the Internet to rule-making at the national level, a growing number of scholars are concerned with governance frameworks and regulatory practices of national or regional authorities (e.g. Daly & Thomas 2017; Massit-Folléa, Méadel & Monnoyer-Smith 2012). They analyse the attempts of states to master the digital transformation through national policies, legislation and regulation. Most of this work takes the form of case studies interested in particular Internet-related policy issues, such as data protection, copyright, net neutrality, content regulation and, increasingly, data regulation (e.g. Busch et al., 2019). Other scholarship in this area comprises cross-national comparative research on specific regulatory issues (e.g. Segurado et al., 2015). A global perspective on these practices and how they relate to the idea of state sovereignty is, however, still missing.

Over the last few years, several IG scholars from various disciplines have shown interest in the notion of digital sovereignty as deployed by state- and non-state actors in a number of political and economic arenas, from more centralised and authoritarian countries to liberal democracies. This literature shows that the term digital sovereignty has a variety of connotations according to different national settings, actor arrangements and the concrete sets of practices related to it (Couture & Toupin, 2019; Pohle & Thiel, 2020). Existing research on these connotations often focuses on past and present imaginaries of digital sovereignty. Some authors trace the discursive changes from the cyber-exceptionalist rejection of states' interference to contemporary sovereignty claims by governments related to IT security, data governance and industry policy (e.g. Mueller, 2020). Others focus on the actors, arguments and ideas behind specific occurrences of the digital sovereignty discourse, e.g. in particular countries or communities (e.g. Ebert & Maurer, 2013). The majority of this research is concerned with sovereignty claims by countries such as China (e.g. Jiang, 2010) and Russia (e.g. Budnitsky & Jia, 2018), but the more recent discourses in European and BRICS countries have begun to receive some attention (e.g. Gurumurthy & Chami, 2016; Keller, 2019; Tréguer, 2017).

The bulk of digital sovereignty research looks at the relationship between statehood and territory and how it is affected by digital networks (e.g. Limonier, 2018; Haggart et al., 2021). The question of how to ensure the self-determination of states and citizens within the borders of their national territory and whether this leads to a "re-territorialisation" or even a "fragmentation" of the Internet is a central theme in this work (e.g. Drake et al., 2016; Mueller, 2017). Scholars also focus on cyber security discourses and policies in order to assess states' efforts to ensure the security of digital infrastructures and the online space related to their national territory (e.g. Kamis & Thiel, 2015). Others, bringing in perspectives in security and surveillance studies, deal with surveillance practices of foreign intelligence agencies or companies and how states seek to craft possible countermeasures (e.g. Tréguer, 2017). In this context, particular attention is paid to state attempts to introduce data localisation laws which limit the storage, movement and/or processing of data to specific geographies and jurisdictions (e.g. Panday & Malcolm, 2018).

Recently, there have been some preliminary attempts to systematise digital sovereignty claims by distinguishing whether they address the capacity for the digital self-determination of states, companies or individuals (Couture & Toupin, 2019; Pohle & Thiel, 2020).

Information systems through the lens of STS and infrastructure studies

A whole tradition in STS has explored during the past few decades the social and organisational dimensions of technical infrastructures, including both material artefacts and their logistical substrata. The core idea of these approaches is that the design of infrastructures is to be understood "systemically" alongside their adoption and (re)appropriation by users, and their imbrication with modes of human organization, in sets of practices that materialize their relational dimension. Embedded, transparent, existing and evolving across space and time, learned by socialization, integrating practical conventions, standards and norms, made visible as they fail and are repaired or cared for – infrastructures keep on questioning STS scholars as they contribute to structure, shape, enable or constrain our "being-together".

Over the years and decades, STS scholars have multiplied and gradually nuanced their approaches to the study of infrastructures, so that a full sub-domain of research, under the *infrastructure studies* banner, is now concerned with the socio-technical infrastructural forms that organize the production, circulation and 'socialization' of knowledge. For the argument put forward by this article, two notions that emphasize the embeddedness of infrastructures in both time and space, while highlighting their evolutionary and systemic qualities, are of particular interest. On the one hand, Barry's (2006) notion of *technological zones* (and more specifically, of infrastructural zones) helps to make sense of spaces within which differences between technical practices, procedures and forms are reduced and common standards are established. The notion alerts to the "need for analysis of the historical construction of particular political and economic spaces, and the specificities of the materials, practices and locations which they transform, connect, exclude and silence". It emphasizes that "the formation of technological zones has become critical to the constitution of a distinction between global/Western political and economic forms and their non-Western others" (Barry, 2006, p. 250), both aspects speaking closely to the aims of the present project. On the other hand, recent work on the concept of *infrastructuring* (Blok et al., 2016; Karasti & Blomberg, 2018) helps to make sense, theoretically and methodologically, of infrastructures as processes, practices and settings that are both expansive and open-ended, even as our starting point as researchers is made of "spatially, temporally and organizationally circumscribed" case-study infrastructures. The shift from infrastructures to *infrastructuring* helps us to account for how a "field is constructed by the engagement of the researcher with the phenomenon of study, and in the process the object of inquiry delineated, if only for the moment" (Karasti & Blomberg, 2018).

Alongside these contributions from the STS tradition, it should be noted that understanding and analyzing infrastructures is a multi-disciplinary endeavor, calling for a cross-fertilization of approaches – especially when addressing the relationship between infrastructures and territories. A foremost example is architect/urbanist Keller Easterling's theorization of infrastructure as "extrastatecraft", the determinant of a set of discreet rules structuring space (2014).

Scholars have elaborated methodological tools to be able to read and narrate infrastructures, such as Star's "ethnography of infrastructure" (1999), calling for an increased ethnographical sensibility to trace what is otherwise in the background, invisible and taken for granted, whose design processes, if empirically tested, can reveal passionate and sometimes confrontational stories of dissonances and attachments (Star & Ruhleder, 1996). Bowker and Star (1999) have labeled as “infrastructural inversion” the double methodological gesture consisting in looking “behind the scenes” of practices to retrace what has been enabled or constrained by design, and in looking “in depth” to enable significations and meaning to emerge from technical standards, devices and apparatuses, so as to understand where conflicts and controversies emerge and how they take shape with infrastructures.

Within this body of work, a particular focus exists on the transformations linked to the deployment of digital technologies in a variety of social worlds (Edwards, 2010). Indeed, when it comes to the Internet and digital technologies, and information systems more broadly, scholars have acknowledged – and empirically analysed – that infrastructure also encompasses more abstract (and a priori immaterial) artefacts, such as protocols, standards (Bowker et al., 2010), software and code (e.g. Fuller, 2008; Blanchette, 2011), alongside the physical infrastructure supporting the functioning of digital networks, such as submarine cables, data centers, Internet Exchange Points (IXPs) and so on. Elaborating on the idea – perhaps most famously summarized by legal scholar Lawrence Lessig’s motto “code is law” – that technical devices can be instruments for social control alongside other normative systems, a number of authors have refined our understanding of the arrangements of power inherent in, and revealed by, technical infrastructures and architectures of the Internet and digital/networked technologies. Exemplars of this research include Galloway’s Foucault-inspired work on TCP/IP and DNS protocols as means of control (2004), DeNardis’ analysis of the “protocol politics” permeating the IPv4 to IPv6 transition (2009), and Gillespie’s analysis of the “relevance of algorithms” in Internet content governance (2014).

The “turn to infrastructure” in Internet governance

Within the lively academic debates overviewed above, STS-informed perspectives examining infrastructures have proliferated; however, they have received comparatively little attention from Internet *governance* scholars until the last decade, with DeNardis (2012) arguably being the scene-setter in this regard. In the past few years, a perspective grounded in both IG research and STS approaches has explored how points of infrastructural control, beyond their originally intended function, can serve as proxies for different actors – first and foremost the state – to regain (or gain) control or manipulate the flow of money, information and the marketplace of ideas in the digital sphere. We have called this set of phenomena, and rising tendency, the “turn to infrastructure in Internet governance” (Musiani et al., 2016). This body of work addresses e.g. the use of the domain name system (DNS) as a tool for intellectual property rights enforcement (Merrill, 2016), the discretionary power of information intermediaries to prioritise strategic interests over privacy commitments in their infrastructural practices (Sargsyan, 2016), or the interplay (and conflict) of technical and political governance in decentralized technologies such as the blockchain that forms the backbone of the Bitcoin cryptocurrency (De Filippi & Loveluck, 2016).

These recent contributions show a shift from a values-in-design approach (Flanagan et al., 2008; i.e., developers and engineers seek to inscribe particular values in the infrastructures they create for them to better carry out their intended functions), to a full-fledged politicisation of IG infrastructures, where a wide range of private and public actors seek to leverage administrative and coordinating functions inscribed in digital infrastructures as instruments of power (DeNardis, 2009). We have observed how the use of Internet infrastructure to carry out functions diverging from their intended, original objective can lead to significant collateral damage to the stability and security of the Internet and the protection of online civil liberties (DeNardis & Musiani, 2016). The “infrastructuring digital sovereignty” perspective elaborates on this past work, observing as a cornerstone of this proposed framework that states pursuing strategies of autonomisation, independence, isolation and strengthening of sovereignty of their national Internets are often engaged in these politicised uses of Internet infrastructure, with the associated risks becoming increasingly evident alongside potential opportunities. STS approaches, with their attention to situated practices and infrastructural agency, are well-suited to bringing these aspects to the foreground – thereby shedding new light on how strategies of digital sovereignty get inscribed in infrastructures, and understanding what this reveals of transformations in institutions and territories.

Approaching Digital Sovereignty Through the “Infrastructuring” Lens

In order to shed new light on how strategies of digital sovereignty get inscribed in infrastructures, and understand what this reveals of transformations in institutions and territories, two main “scholarly gestures”, both theoretical and methodological, are desirable. First, to follow systems and arrangements, grounded in digital infrastructures, where sovereignty as a foundational principle of the nation state is promised, intended, constructed, co-opted. Second, to zoom in to the technical components of digital infrastructure as strategic sites to trace the inscription of particular visions of sovereignty.

As for the first aspect, we build on approaches derived from infrastructure studies – in particular from the concepts of *infrastructuring* (Blok et al. 2016), *infrastructural zones* (Barry, 2006) and *turn to infrastructure* (Musiani et al., 2016) as a foundation to detect emerging infrastructure-based understandings and instantiations of digital sovereignty. This allows us to examine how the label becomes instantiated in a number of macro and micro “infrastructures of control”, how institutional and other actors seek to co-opt them as proxies of their authority, and how this in return re-shapes their identities and the territories in which they operate.

As for the second aspect, the methodological focus on the technical devices and components of Internet infrastructures that enable the construction of digital sovereignty facilitates the understanding of Internet infrastructures as points of interface, contact and control that arrange and materialize underlying relationships. We place the methodological focus on infrastructures as analytical sites in which broader, heterogeneous processes become visible, allowing to detect transformations in the order of authority and the (re-)distribution of power (DeNardis & Musiani, 2016). We need to identify and analyse situations where Internet infrastructures do not merely act as tools, but as actual mediators tasked with the politically-relevant, and never neutral, assignment of translating the management of technical “control points” (DeNardis, 2014) into arrangements of power and definitions of digital sovereignty.

These theoretical and methodological guidelines lay the foundations for taking as an object of analysis the set of processes and practices which I call “infrastructuring digital sovereignty”. By this concept, I refer to the materially and technologically-embedded set of procedures that co-shape, and co-produce, three types of entities:

(1) institutions as *loci* of power, be they States or supra-national entities, as well as hybrids of public institutions and the private sector at different scales;

(2) the territories in which these actors operate;

(3) the plural, grounded notion of digital sovereignty itself.

We can envisage these three as core questions that shape the research agenda for studying digital sovereignty through a perspective blending STS and studies of Internet and digital governance, as well as insights from other disciplines (history of technology, cybersecurity, surveillance studies, political geography). I examine them in turn below.

“Infrastructuring Digital Sovereignty” Shaping Institutional and Hybrid Actors

This question focuses on how institutional boundaries, and the boundaries between institutions and other types of actors (in particular, the private sector) are shaped by infrastructuring processes, and whether as a consequence, new reconfigurations of power, authority and control emerge. This question takes as a starting point the IG scholarly debates, described earlier, concerning the decline in the importance of the nation state and the role of governments and intergovernmental organisations in the global governance system of the Internet. However, a notable shift between the approach presented here and most previous works on this issue is that we are not primarily concerned here with establishing *whether* nation states retain *more or less* control than in the pre-Internet era, but to investigate what particular *loci* of power – institutional or hybrid – are constituted by material activities of infrastructuring. In this regard, work at the crossroads of history of technology and STS, such as Mitchell (1991) on the materially- and technologically-embedded foundations of the French state bureaucracy and, more recently, Zajacz (2019) on the United States’ use of radiotelegraphy as both a new technology and a new corporate form to advance their global position, provide additional guidance in the attempt to develop a “real-time history” of how institutional and hybrid actors are brought into existence and continuously shaped by very material and situated activities such as posing submarine cables, constructing data centers, establishing peering agreements, building a country’s own Domain Name System, pushing for import-substitution policies, and so on.

“Infrastructuring Digital Sovereignty” Shaping National and Supra-National Territories

This question addresses how socio-geographical space is shaped by Internet infrastructures and their subtending networking architectures, to investigate emerging understandings of territory at both the national and supra-national levels. As we have seen above, previous studies of digital sovereignty have addressed the relationship between statehood and territory and how it is affected by digital networks; however, the extent to which this relationship is co-shaped and revealed by digital infrastructuring, and how this affects the conceptualization of territory itself, is yet understudied, a notable exception being the very recent work by Möllers (2021). To address this gap, it will be useful to blend the STS/infrastructure studies theoretical and methodological tools with insights from political geography (e.g. Amoore, 2018), and to converse with ongoing work in STS that examines how data infrastructures and systems for the management of migration fluxes and registration of foreign populations are co-shaping territories and the right to hold citizenship (Pelizza, 2020). This question asks to which extent transformations in States and their sovereignty might be underpinned by infrastructural changes in the conceptualization of space; it asks which conceptualizations of space emerge from networked digital infrastructures, and how they affect the relationship between territory and sovereignty.

“Infrastructuring Digital Sovereignty” Shaping the Notion of (Digital) Sovereignty Itself

This question investigates how reconfigurations of institutions and territories re-shape in return (digital) sovereignty itself, as a “grounded” notion and concept. “Information policy mediates the identity of the nation state” (to paraphrase Braman, 2006, 155), and this in turn shapes the very definition of sovereignty, makes it plural and contextdependent: how do processes of digital infrastructuring re-enact this notion? From the argument that conceived trans-national digital networks as causes of the erosion of sovereignty and decentralization of authority (Castells, 1996), to the conception of digital, networked technologies as a tool for efficiency and competitiveness (Heeks, 2006), the relationship between digital technologies and the form of the nation state has usually been framed in either causal or functional terms. However, with the digitization of state informational assets (Pelizza, 2016), the privatization or hybridization of functions traditionally bestowed upon the state and supra-national organizations (DeNardis, 2014), and the move towards systems of big-data-enabled mass surveillance (Lyon, 2014), the information-based redistribution of authority has become embedded into infrastructures. Taking this scenario into account, we ask here how to account for transformations in old and new *loci* of power, in ways that do not *a priori* assume the roles and identities of sub-, trans- or national agencies, and particular instantiations of their sovereignty, but allow accounting for their re-enactment.

An Ongoing "Pilot Case": How Russia Infrastructures its Digital Sovereignty[4]

Famously unregulated in the 1990s and aughts (Deibert and Rohozinski, 2010). the Russian Internet (RuNet) has begun to face serious national regulation only in the early 2010s (Oates, 2013; Soldatov and Borogan, 2015). In particular, Roskomnadzor (RKN),

[4] This section presents some elements of an ongoing research programme on infrastructure-based practices of digital sovereignty in Russia. Several publications derived from this fieldwork have been published in May 2021 (e.g. Daucé and Musiani, 2021; Ermoshina, Loveluck and Musiani, 2021).

the federal government communications control body[5], has seen its jurisdiction and reach rapidly extended to domains as varied as the control of online content, the right to block websites, and the registering of blocked websites, with a substantially increased possibility of censorship. RKN's control relies on its important nexus of relations and collaborations with actors that maintain and keep the Internet operational, and propose connectivity solutions to users (access providers, owners of digital businesses...).

This scenario has led to a particular and Russia-specific instantiation of the "digital sovereignty" label, which has taken hold in the past decade: indeed, Russian authorities are actively pursuing a digital sovereignty strategy that focuses on an autonomisation of the RuNet through a complex dialectic of law and infrastructure-based enforcement, aimed at countering foreign "influences" and agents, as well as their devices and applications; in the process, Russian authorities are attempting to remove their citizenry, as much as possible, from the contingencies and dependencies of a hyperconnected world. Exemplars of this tendency are what have become known as the *Sovereign Internet law*, adopted in 2019 with the official aim of protecting the country from cyberattacks, and the *law against Apple*, passed in 2020 with the objective of having all smartphone devices in Russia to preload a host of 'Russian-made' applications.

Since early 2018, the *ResisTIC (Criticism and circumvention of digital borders in Russia)*[6] project team endeavors to analyze how different actors of the RuNet resist and adapt to the recent wave of centralizing regulations, with a particular focus on online resistance that reveals so far lesser-known social practices and techniques for

[5] RKN is also the data protection regulator in the country; it is not an independent authority, but a governmental agency (federal service) established under the Ministry of ICTs and Media.

[6] https://www.resistic.fr

circumventing online constraints. These circumventions echo a long history of social inventiveness in the last decades of the Soviet period, when many Soviet citizens routinely transgressed and reinterpreted the norms and rules of the socialist state, especially in their use of communication infrastructures (Yurchak, 2013; Peters, 2016; Zakharova, 2020).

One of the project's primary objectives is to explore the extent to which control and circumvention strategies are embedded in, and conducted by means of the RuNet infrastructure; our aim has been to shed light on the complex relationship between technical devices, algorithms and infrastructures (Brousseau, Marzouki and Méadel, 2012) in the Russian digital sphere, and the politics and markets taking shape in the country. As the project moves towards its conclusion, we are reflecting on the implications of fieldwork carried out by the project team at the crossroads of digital sovereignty, data and infrastructure – both its development and its uses, oftentimes very creative and subversive. The Russian case is understood as a "laboratory" of broader tendencies in Internet governance worldwide (Daucé and Musiani, 2021).

In the past three years, the project team has undertaken an infrastructure-based sociology of the RuNet, focusing on the technical devices and assets involved in surveillance and censorship, and on the strategies of resistance and circumvention "by infrastructure" that follow. Our fieldwork sites have ranged from the emblematic "Telegram ban" and its socio-technical ramifications unveiling tensions between the "sovereign Internet" governmental narrative and infrastructure-based resistance practices (Ermoshina and Musiani, 2021) to the political bias-related controversies surrounding the Yandex.News aggregator (Daucé and Loveluck, 2021), and from the paradox related to the use of Google services in Russia, which sees several Russian NGOs considering the Internet giant as a protector of civil liberties (Bronnikova and

Zaytseva, 2021) to the particular definitions of freedom and circumvention enacted by shadow mass-literature online libraries, made illegal in 2013 (Ostromooukhova, 2021).

Our different fieldwork observations have both responded to, and contributed to further build and consolidate, the research agenda outlined above, which now calls for a wider and comparative research programme. For the time being, let us briefly examine some elements related to the three questions, as they shed light on the Russian case (see for more details Daucé and Musiani, 2021 and Ermoshina, Loveluck & Musiani, 2021).

First, how does “infrastructuring digital sovereignty” shape institutional and hybrid actors of the RuNet? This research question, as we recall, prompts to move away from the issue of whether the Russian state has been able to increase its power (or not) by means of the recent regulation wave, and focus instead on how material activities of infrastructuring are constituting particular loci of power. Our fieldwork has revealed several instances where this is happening. We examined, e.g., how the implementation of different types of “black boxes” by Russian Internet Service Providers (ISPs), as the private technical intermediaries ensuring the routing of Internet traffic towards end users, has been spurred by recent legislation and has engendered, in parallel, several circumvention techniques. We also investigated the technical choices made by developers of “Russian tech” national champions, such as the search engine Yandex, and how these choices have co-shaped a complex power network of media players, news professionals, authorities and platform developers that strongly impacts how information reaches Russian citizens.

The second question addresses whether socio-geographical space is shaped by Internet infrastructures, and how this affects the conceptualization of territory itself, thereby shifting from the “traditional” question of whether statehood has been reduced by digital networks and would now be “returning”. Our fieldwork in the Russian case shows the very high degree of interdependence of the RuNet across national borders and at all protocol levels; unlike China, which has designed its network with a very specific project of centralised internal governance, Russia has more than 3,000 ISPs and a complex branched-out infrastructure with multiple physical and economic connections with foreign countries. In this context, it is very difficult for ISPs and other Internet operators to know exactly how and to what extent they depend on other infrastructure components (traffic exchange points, content distribution networks, data centers etc.) located beyond their borders, which complicates the understanding of “territory” as it relates to the RuNet and affects, in particular, its ability to isolate itself from the rest of the digital world, which is an explicit goal of its digital sovereignty strategy.

Finally, how is the notion of digital sovereignty itself re-enacted by processes of digital infrastructuring, beyond the image of it that the Russian state seeks to project and its purported “linearity”? Indeed, drawing these different cases of “infrastructuring digital sovereignty” together provides a non-linear, nuanced and complex understanding of the specificities of Russian Internet governance, that challenges the national conception of digital sovereignty, often described as a strictly centralized, top-down and efficient information control system. Our case studies have proposed to pay attention to micro-techniques of circumvention and shows how the discourse on Internet sovereignty (and the subsequent demand for all information control technologies to be “made in Russia”) is currently giving way to two important paradoxes in the country. On the one hand, it can lead groups of activists and users whose main priority is to evade the Russian government’s surveillance, control and sovereignty to end up spontaneously subjecting themselves to other forms of surveillance, control and sovereignty, notably originating in the United States. On the other hand, it opens up technical and legal opportunities for mundane resistances and the existence of “parallel” RuNets, where particular instantiations of informational freedom are still possible.

Conclusions

Infrastructure speaks to vital *material* sovereignty questions. In this article, I have made a case, and outlined an agenda, for studying the concept of (digital) sovereignty via the infrastructure-embedded “situated practices” of various political and economic projects which aim to establish autonomous digital infrastructures in a hyperconnected world. This contribution is primarily a call for a wider and comparative research programme in the years to come, and seeks to establish a research agenda to move forward in this direction; however, the last part of the article has focused on Russia as a pilot case, subject of an ongoing research project, and an empirical testbed for the framework proposed in the article.

The article has proposed the notion of “Infrastructuring Digital Sovereignty” as a conceptual innovation at the crossroads of sociological processes (organizing, acting towards political goals), processes of sense-making and interpretation (fleshing out the significance of notions such as sovereignty and territory) and socio-technical practices (handling and management of Internet infrastructures as key mediators). The article suggests, with insights from STS, that advancements in our understanding of digital sovereignty can be brought about by making sense, theoretically and methodologically, of infrastructures as *infrastructur-ing* – as processes, practices and settings that are expansive, evolving, and open-ended. Infrastructure-based perspectives also bring to our understanding of digital sovereignty a material and performative lens that understands actors (including institutions) not as given a priori, and their outputs not as *faits accomplis* (Flyverbom, 2011), but as the result of evolutionary techno-social activities.

Yet, to fully grasp digital sovereignty – digital sovereignties – as infrastructuring processes, STS and infrastructure studies cannot, of course, operate in a "scholarly vacuum". They need surveillance studies, to investigate how arrangements of power are enacted through technical devices and systems, and political geography to bring in methodological tools that focus on the conceptualizations of space embodied by digital infrastructures. Finally, Internet governance studies informed by political science, international relations and international law, and by history of technology, help inform the exploration of long-term processes such as the erosion and reaffirmation of state authority, and state "reassembling" as they relate to the Internet and digital technologies.

According to many commentators, the quest for digital self-determination will be a central geopolitical issue in the coming decade. "Digital sovereignty" is an increasingly crucial component not only of states' Internet governance strategies, but of the very essence of their founding principles such as territoriality and authority. Public and private actors worldwide are making a case that (digital) sovereignty is necessary to protect fundamental societal "goods" including economic prosperity, security, and culture. The concept of digital sovereignty is expected to acquire even greater relevance in the coming years, with widespread deployment of technologies such as the Internet of Things and artificial intelligence. This requires to develop not only new governance solutions, but also innovative knowledge paradigms. The systemic transformations brought about by the "digital sovereignty wave" worldwide, in its variety of instantiations, must also be addressed as sets of practices of social ordering, intimately linked to how humans and organizations build, develop, use, co-opt and resist digital infrastructures.

Acknowledgments

This work has received funding from the French National Agency for Research (Agence Nationale de la Recherche, ANR) in the frame of the project ResisTIC (Les résistants du net. Critique et évasion face à la coercition numérique en Russie, ANR-17-CE26-0020).

References

Amoore, L. (2018). “Cloud geographies: Computing, data, sovereignty”, *Progress in Human Geography, 42*(1), 4-24.

Barry, A. (2006). “Technological zones”, *European Journal of Social Theory*, 9(2), pp. 239-253.

Bijker, W. E. (1995). *Of Bicycles, Bakelites, and Bulbs. Toward a Theory of Sociotechnical Change*. Cambridge, MA: MIT Press.

Blanchette, J.-F. (2011). “A material history of bits”, *Journal of the Association for Information Science and Technology*, 62, pp. 1042–1057.

Blok, A., Nakazora, M. & Winthereik, B. R. (2016). “Infrastructuring Environments”, Science as Culture, 25 (1), pp. 1-22, https://doi.org/10.1080/09505431.2015.1081500

Bowker, G.C., Baker, K., Millerand, F. & Ribes, D. (2010). “Toward Information infrastructure Studies: Ways of Knowing in a Networked Environment”, in J. Hunsinger (Ed.), *International Handbook of Internet Research*. Springer.

Bowker, G. C. & Star, S. L. (1999). *Sorting Things Out: Classification and its Consequences*. Cambridge, MA: The MIT Press.

Braman, S. (2006). *Change of State: Information, Policy, and Power*. Cambridge, MA: The MIT Press.

Bronnikova, O., & Zaytseva, A. (2021). ‘In Google we trust’? The Internet giant as a subject of contention and appropriation for the Russian state and civil society. *First Monday*, 26(5).

Brousseau, E., Marzouki, M., & Méadel, C. (Eds.). (2012). *Governance, regulation and powers on the Internet*. Cambridge University Press.

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

Busch, A., Breindl, Y., Jakobi, T. (Eds., 2019). *Netzpolitik: Ein Einführender Überblick*. Springer VS, Wiesbaden.

Castells, M. (1996). *The Rise of the Network Society: The information age: Economy, society, and culture*. Vol. 1. Oxford: Blackwell Publishing.

Couture, S. & Toupin, S. (2019). “What does the notion of “sovereignty” mean when referring to the digital?”, *New Media & Society*, 21, 18. https://doi.org/10.1177/1461444819865984

Daly, A. & Thomas, J. (2017). Australian Internet Policy. *Internet Policy Review* 6. https://doi.org/10.14763/2017.1.457

Daucé, F., & Loveluck, B. (2021). Codes of conduct for algorithmic news recommendation: The Yandex.News controversy in Russia. *First Monday*, *26*(5). https://doi.org/10.5210/fm.v26i5.11708

Daucé, F. and Musiani, F., eds. (2021). Infrastructure-Embedded Control, Circumvention and Sovereignty in the Russian Internet. *First Monday*, 26(5).

De Filippi, P. & Loveluck, B. (2016). “The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure”, *Internet Policy Review*, 5. https://doi.org/10.14763/2016.3.427

Deibert, R.J. & Crete-Nishihata, M. (2012). “Global Governance and the Spread of Cyberspace Controls”. *Global Governance*, 18, pp. 339–361. https://doi.org/10.5555/1075-2846-18.3.339

Deibert, R., and Rohozinski, R. (2010). “Control and Subversion in Russian Cyberspace.” Pp. 15–34 in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, MA: MIT Press.

DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

DeNardis, L. (2012). “Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance”, *Information, Communication & Society*, 15, pp. 1–19.

DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA: The MIT Press.

DeNardis, L. & Musiani, F. (2016). “Introduction: Governance by Infrastructure”, in Musiani, F., Cogburn, D.L., DeNardis, L., Levinson, N.S. (Eds.), *The Turn to Infrastructure in Internet Governance,* New York: Palgrave Macmillan, pp. 3–21.

Drake, W.J., Cerf, V.G., Kleinwächter, W. (2016). “Internet Fragmentation: An Overview”, Future of the Internet Initiative White Paper, World Economic Forum, Geneva.

Easterling, K. (2014). *Extrastatecraft: The Power of Infrastructure Space*. Verso Books.

Ebert, H. & Maurer, T. (2013). “Contested Cyberspace and Rising Powers”, *Third World Quarterly*, 34, pp. 1054–1074. https://doi.org/10.1080/01436597.2013.802502

Edwards, P. N. (2010). *A vast machine: Computer models, climate data, and the politics of global warming*. Cambridge, MA: The MIT Press.

Elden, S. (2005). “Missing the point: globalization, deterritorialization and the space of the world”, *Transactions of the Institute of British Geographers*, 30, pp. 8–19. https://doi.org/10.1111/j.1475-5661.2005.00148.x

Epstein, D., Katzenbach, C. & Musiani, F. (2016). Doing internet governance: practices, controversies, infrastructures, and institutions. *Internet Policy Review*, 5(3). DOI: 10.14763/2016.3.435

Ermoshina, K., Loveluck, B., & Musiani, F. (2021). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. *Journal of Information Technology & Politics*, 1-16.

Ermoshina, K., & Musiani, F. (2021). The Telegram ban: How censorship “made in Russia” faces a global Internet. *First Monday*, *26*(5).

Flanagan, M., Howe, D.C., Nissenbaum, H., (2008). “Embodying values in technology: Theory and practice”, *Information Technology and Moral Philosophy*, 322

Flyverbom, M. (2011). *The power of networks: Organizing the global politics of the Internet*. Cheltenham, UK: Edward Elgar Publishing.

Fuller, M. (2008, ed.). *Software Studies: A Lexicon*. Cambridge, MA: The MIT Press.

Galloway, A. R. (2004). *Protocol: How control exists after decentralization*. Cambridge, MA: The MIT Press.

Gillespie, T. (2014). “The relevance of algorithms”, in T. Gillespie, P. J. Boczkowski and K. A. Foot (eds.), *Media technologies: Essays on communication, materiality, and society*. Cambridge, MA: The MIT Press.

Goldsmith, J. & Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World*, New York: Oxford University Press.

Gurumurthy, A. & Chami, N. (2016). “Internet governance as “ideology in practice” – India’s “Free Basics” controversy”, *Internet Policy Review*, 5.

Haggart, B., Tusikov, N., & Scholte, J. A. (Eds.). (2021). *Power and Authority in Internet Governance: Return of the State?* Routledge.

Heeks, R. (2006). *Implementing and managing eGovernment: an international text*. Sage.

Hofmann, J. (2016). “Multi-Stakeholderism in Internet Governance: Putting a Fiction into Practice”, *Journal of Cyber Policy*, 1, pp. 29–49.

Hofmann, J., Katzenbach, C. & Gollatz, K. (2017). “Between Coordination and Regulation. Finding the Governance in Internet Governance”, *New Media & Society*, 19, pp. 1406–1423.

Jiang, M., (2010). “Authoritarian Informationalism: China’s Approach to Internet Sovereignty”, *SAIS Review of International Affairs*, 30, pp. 71–89.

Johnson, D.R. & Post, D. (1996). “Law and Borders: The Rise of Law in Cyberspace”, *Stanford Law Review*, 48, pp. 1367–1402.

Kamis, B. & Thiel, T. (2015). “The Original Battle Trolls: How states represent the Internet as a violent place”, Working Paper n°23, Peace Research Institute Frankfurt, http://thorsten-thiel.net/wp-content/uploads/2017/09/Kamis-Thiel-2015-The-Original-Battle-Trolls.pdf

Karasti, H., & Blomberg, J. (2018). “Studying infrastructuring ethnographically”, *Computer Supported Cooperative Work*, *27*(2), pp. 233-265.

Keller, I. C. (2019). *Regulação nacional de serviços na Internet: exceção, legitimidade e o papel do Estado*. Editora LumenJuris, Rio de Janeiro.

Klein, H. (2002). “ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy”, *The Information Society*, 18, pp. 193–207.

Lessig, L. (2006). *Code 2.0*. New York: Basic Books.

Limonier, K. (2018). *Ru.net: géopolitique du cyberespace russophone*. Editions L’Inventaire.

Lyon, D. (2014). Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big data & society*, *1*(2).

Malcolm, J. (2008). *Multi-Stakeholder Governance and The Internet Governance Forum*. Terminus Press, Perth.

Massit-Folléa, F., Méadel, C., Monnoyer-Smith, L. (2012, eds.). *Normative Experience in Internet Politics*. Paris, Presses des MINES.

Merrill, K. (2016). "Domains of Control: Governance of and by the Domain Name System", in: Musiani, F., Cogburn, D.L., DeNardis, L., Levinson, N.S. (Eds.), *The Turn to Infrastructure in Internet Governance*. Palgrave Macmillan, New York, pp. 89–106.

Mitchell, T. (1991). "The limits of the state: beyond statist approaches and their critics", *The American Political Science Review,* 85 (1), pp. 77-96.

Möllers, N. (2021). "Making Digital Territory: Cybersecurity, Techno-nationalism, and the Moral Boundaries of the State", *Science, Technology, & Human Values*, *46*(1), pp. 112-138.

Mueller, M. (2020). "Against Sovereignty in Cyberspace", *International Studies Review*, *22*(4), pp. 779-801.

Mueller, M. (2017). *Will the Internet Fragment? Sovereignty, Globalization and Cyberspace*. Cambridge, UK: Polity.

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

Musiani, F., Cogburn, D.L., DeNardis, L., Levinson, N.S. (2016, eds.). *The Turn to Infrastructure in Internet Governance*, New York, NY: Palgrave Macmillan.

Oates, S. (2013). *Revolution Stalled: The Political Limits of the Internet in the Post-Soviet Sphere*. Oxford: Oxford University Press.

Ostromooukhova, B. (2021). "Free libraries for the free people": How mass-literature "shadow" libraries circumvent digital barriers and redefine legality in contemporary Russia. *First Monday,* 26(5).

Panday, J. & Malcolm, J. (2018). "The Political Economy of Data Localization", *Partecipazione e conflitto*, 11, pp. 511–527.

Pelizza, A. (2020). "Processing alterity, enacting Europe: Migrant registration and identification as co-construction of individuals and polities", *Science, Technology, & Human Values*, *45*(2), 262-288.

Pelizza, A. (2016). "Developing the vectorial glance: infrastructural inversion for the new agenda on government information systems", *Science, Technology, & Human Values*, *41*(2), 298-321.

Peters, B. (2016). *How not to network a nation: The uneasy history of the Soviet Internet*. Cambridge, MA: The MIT Press.

Pohle, J., & Thiel, T. (2020). “Digital sovereignty”, *Internet Policy Review*, *9*(4).

Raboy, M., Landry, N., Shtern, J. (2010). *Digital Solidarities, Communication Policy and Multi-Stakeholder Global Governance: The Legacy of the World Summit on the Information Society*. New York: Peter Lang.

Sargsyan, T. (2016). “The privacy role of information intermediaries through self-regulation”, *Internet Policy Review*, 5, https://doi.org/10.14763/2016.4.438

Schafer, V. (2015). “Part of a whole: RENATER, a twenty-year-old network within the Internet”, *Information & Culture*, 50, pp. 217–235.

Segurado, R., Lima, C.S.M. de, Ameni, C.S. (2015). « Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França », *História, Ciências, Saúde-Manguinhos*, 22, pp. 1551–1571. https://doi.org/10.1590/S0104-59702014005000015

Soldatov, A., and Borogan, I. (2015). *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*. New York: PublicAffairs.

Star, S. L. (1999). “The Ethnography of Infrastructure”, *American Behavioral Scientist,* 43 (3), pp. 377-391.

Star, S. L. & Ruhleder, K. (1994). “Steps towards an ecology of infrastructure: Complex problems in design and access for large-scale collaborative systems”, in *Proceedings of the Conference on Computer Supported Cooperative Work*, Chapel Hill, NC: ACM Press, pp. 253–264.

Tréguer, F. (2017). “Intelligence Reform and the Snowden Paradox: The Case of France”, *Media and Communication*, 5, https://doi.org/10.17645/mac.v5i1.821

Yurchak, A. (2013). *Everything was forever, until it was no more: The last Soviet generation*. Princeton: Princeton University Press.

Zájacz, R. (2019). *Reluctant Power: Networks, Corporations, and the Struggle for Global Governance in the Early 20th Century*. Cambridge, MA: The MIT Press.

Zakharova, L. (2020). *De Moscou aux terres les plus lointaines. Communications, politique et société en URSS*. Paris : EHESS.