Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case
by Polina Kolozaridi and Dmitry Muravyov

Abstract
In reference to Russia, the concept of “Internet sovereignty” is commonly used to evoke the state’s efforts to tighten its control over the Internet in order to consolidate a non-democratic political regime. Many scholars have discussed Russia’s “sovereign Internet law,” adopted in 2019, yet the precise meaning of both “sovereign” and “Internet” in this context has largely been overlooked. In this article, we attempt to problematize the use of both concepts by drawing on the history of the Internet in Russia to accentuate the structural asymmetries of power in “global” Internet governance. We argue that Russia’s Internet sovereignty claims, grasped in the context of these asymmetries, can be seen as an expression of counter-hegemonic tendencies. Moreover, a historical account of the Internet’s transformation in Russia problematizes a conception of “Internet sovereignty” as unitary and unchanging.

Contents
Introduction
Sovereignty and the Internet: Entangled and decoupled
Russia, the Internet, and the state
Reassembling sovereignty and the Internet?
Conclusion: Broadening research focus in studies of Internet governance

Introduction
As a matter of public concern, the “sovereign Russian Internet” regulation is widely believed to be closely linked to Russia’s contemporary political regime and its increasingly fraught foreign policy relations with the West. Scholars, journalists, politicians, and activists, both domestic and foreign, frequently articulate their anxieties about the government’s plans to cut Russia off from the global Internet network (Asmolov, 2010; Tselikov, 2014; Maréchal, 2017; Soldatov, 2019).

Yet conceptions of the Internet, Russian governance, and “sovereignty” have all changed over the course of the past three decades — the era in which the Internet became a focus of public concern. It is thus important to problematize the research approaches used in discussions of the dynamics of Internet policy in Russia, making them sensitive to changes that occurred with main concepts through time.

Our analytical aim in this paper is to propose a reconsideration of the different legacies and scales that have
co-shaped the transformation of Internet regulation in Russia. The proposed reconsideration proceeds in three steps. First, we determine and clarify the key concepts employed in discussions on Internet sovereignty. Second, we draw attention to those aspects of Internet history in Russia that are often overlooked in scholarly and public discussions about Internet sovereignty. Third, in linking the two previous arguments, we propose that a more nuanced understanding of Internet sovereignty can carve out a space for alternative interpretations of the dynamics of Internet policy. Although this paper’s primary focus is Internet sovereignty within Russia, we believe that its argument can serve as a point of departure for other local and national cases, as the fragmentation of the Internet is now widely discussed in Internet governance research (e.g., Mueller, 2017, 2010).

We begin with a problematization of the terms “sovereignty” and “Internet” through the prism of a theoretical and historical analysis. Our aim is to underscore the ways in which the Internet can be construed simultaneously as global, transnational, national, and local — as well as both material and ideational. Accounting for these multiple scales problematizes scholarly discussions of Internet sovereignty. Following this, we contextualize Internet sovereignty within debates in the field of Internet governance.

In the second section, we argue that the Internet’s historical transformation and its (regional, national) context influence discussions on Internet sovereignty. Here, we introduce and contextualize the concept of “nets” (Driscoll and Paloque-Berges, 2017) as an alternative to the prevalent discourse about a single, united and centralized Internet in Russia. Simultaneously, we question whether the “RuNet” is a useful term to speak about the Internet in Russia.

In the final section of the article, we call for a reconsideration of claims to “Internet sovereignty” through attentive readings of national and local Internet histories, as well as of the global arrangements of Internet governance.

Sovereignty and the Internet: Entangled and decoupled

The Internet has always stood in a complicated relationship with state sovereignty. Early Internet utopias, such as Barlow’s “Declaration of the independence of cyberspace”, proclaimed it a stateless space and contended that its governance should not adhere to the laws of national governments. The Internet of the 1990s and early 2000s was imagined as a universal technology that made global connectivity possible beyond the borders of nation-states (Turner, 2010; Flichy, 2007). Such assumptions were variously rooted in digital communities research (see the summary and critique in Pelizza, 2018), diaspora studies, or coding practices (Joyce, 2010). In scholarly discussions, the relationship between sovereignty and the Internet has been situated in the context of globalization — loosely speaking, the idea of social, economic, and political integration across multiple states and regions of the world (Sassen, 1998).

The globalization of that era was also framed as a comprehensive and world-historical process, insofar as the Cold War had ended and the USSR dissolved. For those in the post-Soviet countries, this meant that new identities could be forged and internalized, as people stayed connected. In an era of sweeping social changes, people moved across the former USSR republics and many repatriates and diaspora communities migrated to Israel, Germany, Greece, and other countries [1]. While this process has been thoroughly studied, the question of Internet usage in the context of these movements remains underexplored and eclipsed by apparently Western European and Atlantic “grand narratives” about the period as marked by the rise of networks and globalization.

The idea of multi-stakeholder Internet governance also inherits this particular vision of the Internet as a global phenomenon. It presupposes that the Internet is a transnational matter of concern that requires an inclusive set of decision-makers for its regulation. The core set of stakeholders comprises states, businesses, and civil society organizations (Dutton, 2015), and occasionally academics. The Internet Governance Forum [2], for example, replicates the same principle on both global and the national levels. However, it should be
underscored that plenty of stakeholders are often excluded from this “core list,” among them free software developers, designers, moderators of online public groups, and others.

**The Internet beyond a global network**

The ways in which Internet regulation has been sustained and reproduced are complex and have shifted over the years and decades. Alongside the legacy of utopian visions of cyberculture, regulation has developed across different cultures and countries and been adapted to the particular needs of communities, organizations, and individuals.

Scholars have become increasingly critical of a “mainstream global history” (Russell, 2017; Turner, 2017) of the Internet originating in, and focused upon, the United States. A similar critique has been levelled against narratives surrounding the Internet’s present state (Goggin and McLelland, 2017). Valérie Schafer summarizes these critical initiatives as attempts at writing a transnational history, while stressing that this need not necessarily imply fragmentation, but rather an “articulation of [the] local and [the] global” and a rethinking of the object of research [3].

Heeding this critique, we combine two different perspectives in our consideration of the Internet. First, we consider the Internet as a transnational and cross-border network with physical infrastructure that is situated within various states’ borders. As physical infrastructure, the Internet is always bounded by territories and spatially situated within particular states’ jurisdictions, from ISP equipment to data centers. In our view, it is crucial to account for how the Internet can be governed at the level of alterations to physical infrastructure(s), prompted not only by legislative changes but also by seemingly innocuous technical tweaks. Multifaceted research efforts by scholars from different disciplines, notably science and technology studies (STS), have amply demonstrated how the Internet’s infrastructure can be both a site and an object of governance and regulation (Musiani, *et al.*, 2016). The infrastructure layer of the Internet, as will be demonstrated in the second section of this paper, is crucial for understanding Internet sovereignty in Russia.

Second, the Internet is a worldwide network that engages utopian visions of globalized countries, organizations, and communities with porous borders. Due to this ambiguity, the Internet poses a challenge for sovereignty in different ways. We cannot explain the nature of this challenge by strictly and unproblematically distinguishing between the “technical” and the “social,” the “material,” and the “ideational,” as they are inextricably entangled and form an integral part of the Internet as a phenomenon. This has been repeatedly stressed in key handbooks and articles within the field of Internet studies (Dutton, 2013).

Moreover, as an object of governance the Internet is both global and transnational (or cross-border if we choose to emphasize frontiers and the act of crossing them). However, these two words convey different meanings. Transnational, as opposed to global, implies that the Internet surpasses borders yet does not necessarily create something beyond them. Accordingly, insofar as it is global, the Internet could well defy all the “weary giants of flesh and steel” (Barlow, 1996) and foster a global and/or trans-local togetherness. And yet Internet governance remains based upon a coordination between global and local authorities. On the one hand, it is almost never a question of whether governments can legitimately regulate the Internet at all; instead, we face the question of what kind of Internet regulations would be acceptable by the public and the international community. On the other hand, the relationship between digital technologies and states internal politics is an increasingly contentious matter. While some argue that the Internet has significant potential for democratic politics, others point out that it can also be used to support the functioning of non-democratic regimes (Boas, 2006). Discussions on Internet sovereignty now largely pivot around arguments in favor of the primacy of the state in governing the Internet (Goldsmith and Wu, 2006) or around support for alternative models, most notably what has come to be referred to as “multistakeholderism” (DeNardis, 2014; Mueller, 2017, 2010).

In the imaginaries of international journalists, scholars, and the public at large, Russia, together with China, is considered to be emblematic of what Polatin-Reuben and Wright (2014) have termed “strong sovereignty.” In their examination of approaches to digital sovereignty in BRICS countries, they oppose Brazil, India, and
South Africa to Russia and China by proposing a distinction between “weak” and “strong sovereignty”: whereas the former refers to private sector efforts to promote digital rights and data protection, the latter primarily refers to the state’s agenda to preserve national security in cyberspace.

Given how prevalent the term “sovereign Internet” has become among journalists, practitioners, and academics, we would like to inquire deeper into its meaning by way of a historical contextualization of the Russian case in Internet governance debates. This will be our objective in the sections that follow.

**Governance and the normative regulation of the Internet**

Broadly speaking, sovereignty is a controversial and multi-faceted concept, which is used in relation to digital technologies in numerous ways. Couture and Toupin’s (2019) analysis of “digital sovereignty” as a concept reveals that it is currently employed by a variety of actors with somewhat contrasting meanings. States, social movements, indigenous communities, individuals, and grassroots tech collectives evoke sovereignty to connote ideas of self-determination, autonomy, independence, capacity to innovate, or to secure their privacy in the face of external threats. Such an analysis indicates that researchers should be attentive to the plurality of significations embedded within sovereignty as a concept and should critically interrogate how it is used in a given setting.

In parallel, “Internet sovereignty” in the context of global Internet governance is often evoked to signify states’ intentions to contest transnational institutions of Internet governance, such as WGIF, IGF, or ICANN. For example, Mueller (2010) distinguishes between two axes of Internet governance: the networking-hierarchy axis and the nation-state axis. For some analysts, Russia may fall under Mueller’s category “cyber-reactionaries” who favor the predominance of state actors within hierarchical forms of organization.

Networked liberalism, as advocated by Mueller, is tied to normative evaluations of the status quo, as it helps to ensure “open information resources, such as for education and learning, the protection of personal privacy, freedom from surveillance, and rights to expression in an increasingly digital world” (Dutton, 2015). For example, the Internet Governance Forum uses the formulation that “these fragmented regulatory policies across nations can be disruptive for the Internet as a global network” (Internet Governance Forum [IGF], 2018).

Nowadays, as some scholars argue, transnational institutions frequently face significant challenges as multiple nation states manifest their desire to control the Internet. According to this argument, states’ excessive interventions in managing the Internet’s technical infrastructure could threaten the Internet’s stability and thus undermine its global outreach.

This reasoning implies that “the global Internet” is (or should be) preserved against “fragmentation” (Kourandi, *et al.*, 2015) and “balkanization” (Hill, 2012). Such an assumption often refers to technical structures rather than explicitly political or moral values; however, the boundary between these is, once again, rather subtle. So, for example, many such publications preclude any consideration of the prospective positive outcomes of a “balkanized” Internet yet are quick to identify attendant risks. These include “government censorship programs, powerful commercial interests, concerns over cybersecurity, and other dynamic changes in the Internet ecosystem are pulling the global network apart into various distinct, idiosyncratic Internets, threatening the global communication, economic prosperity and innovation the Internet has fostered over the past two decades.” [4] These include “government censorship programs, powerful commercial interests, concerns over cybersecurity, and other dynamic changes in the Internet ecosystem are pulling the global network apart into various distinct, idiosyncratic ‘Internets,’ threatening the global communication, economic prosperity and innovation the Internet has fostered over the past two decades” (Hill, 2012). In other instances, the “risks” attendant to fragmentation or balkanization refer to clusters of associated values, among them “net neutrality” and consumer benefits for users (Kourandi, *et al.*, 2015).

We may contrast this latter perspective with notions of the sovereign Internet in Indian country, as elaborated by Marisa Elena Duarte (2017). Duarte explores the Indian Internet as a decolonial project and as an
infrastructure for establishing an autonomous communication network. In this context, a controversy emerges that is not only technological, but also political, regarding the normativity that underpins claims to sovereignty by indigenous people. Conflicts may arise around the normative acceptability of different approaches to digital self-governance.

The consequences for a conceptualization of nation states’ Internet sovereignty is that once indigenous people’s claims to sovereignty are deemed legitimate, it is no longer possible to argue that aspirations to sovereignty are politically and normatively undesirable per se. An acceptance of the former proposition necessitates a deeper inquiry into which kinds of sovereignty claims and interventions are taken to be “acceptable.” To approach this question, we propose to examine not only states’ actions, but also the underlying governance structures and mechanisms that constitute Internet governance. This latter point will be elaborated in the third section of this paper.

Moreover, the various forms of state intervention concern different aspects of the Internet as a complex socio-technical object. For example, several of the contributions to the volume *The turn to infrastructure in Internet governance* (Musiani, *et al.*, 2016) have demonstrated that states’ control over the Internet is now significantly shaped by *ex ante* means of infrastructural changes, rather than *ex post* legislation. In an analysis of the “geopolitics of information control,” Deibert [5] has argued that although “the Internet helped unleash non-territorial forces and flows that have helped redefine the landscape of global politics, the Internet’s architecture is now being hotly contested and an object of competing discourses and practices of securitization.”

All in all, these changes to national Internet policies present a challenge for the future of global Internet governance, especially when it comes to grasping the end goal of these interventions from these states’ perspectives. Mueller (2017), for instance, suggests that the problem is not the Internet’s technical fragmentation, given that network effects offer compelling economic benefits to nation states. Instead, in Mueller’s view, the public should construe discussions on fragmentation as “the problem of alignment.” This engages nation states’ political efforts to match the juridical borders of the state with those borders that exist in cyberspace.

The impetus behind such an alignment may be interpreted through the prism of what Möllers (2021) has called the making of “digital territory.” Here, the Internet becomes yet another technology and infrastructure that is critical for the continuation of statecraft across many contemporary polities. Möllers’ empirical research on Germany’s Internet policy persuasively demonstrates how the Internet has been re-imagined as a “national space” of government concern, both materially and morally; one that is replete with specific political imaginaries that in many ways decouple it from the idea of a borderless, global, and universal Internet.

We draw together the contrasting cases of Indian country and Germany to cast light on how the notion of Internet sovereignty transforms together with its context (whether it be indigenous group or nation state). In advancing our argument, we would like to tie together Möllers’ (2021) idea of understanding national Internet policies as a project of the making of “digital territory” with contemporary discussions surrounding Internet sovereignty. Building upon this, we will argue that interpreting developments in Internet policy as though both “sovereignty” and the “Internet” are universal and unchanging phenomena runs the risk of misconstruing the causes behind particular changes.

In the following section, we unravel the transformations of “sovereignty” and the “Internet” in Russia. Here, we turn to the social and political context of the Internet in Russia and point to several events which are, from our perspective, crucial to an understanding of recent and under-examined policy developments.
This section proposes an alternative to existing perspectives on the context of Internet regulation in Russia. In doing so, our aim is not to present an all-encompassing and comprehensive history. Rather, our aim is to draw together several episodes that problematize some of the existing claims regarding Internet sovereignty in Russia and that have often been underexamined. They also extend the context of these claims beyond the peculiarities of the contemporary political regime. To begin with, we argue that the Russian state’s comparatively late interest in the Internet (e.g., in contrast to the United States or China) fostered a multiplicity of “net histories,” which have since become politically dormant and yet remain important for a nuanced understanding of Internet sovereignty in Russia. We then proceed to problematize one of the main models in global Internet governance, multistakeholderism, by paying close attention to the variety of Internet stakeholders in Russia.

“Late interest” refers to the marked absence of state projects or particular laws for Internet regulation in Russia throughout the 1990s and early 2000s. While there were some attempts to regulate specific spheres, as well as to extend Internet access to various cities and rural areas, these initiatives were not centralized.

**Russian Internet sovereignty**

From its inception, the Internet has presented both a challenge and an opportunity to rethink the concept of sovereignty. Now more than ever, the problematic has become topical in the Russian context, in light of what journalists, researchers, and some Internet activists refer to as the country’s 2019 “sovereign Internet” law — the trend and the term itself appeared much earlier (Asmolov, 2010; Stadnik, 2019). Those who have coined this term have largely cast a series of legislative initiatives and rhetorical framings of the Internet as a coordinated attempt to “control” cyberspace and to strengthen nation states’ capacities to enforce that control.

Several researchers have proposed a more complex reading and argue that “Internet governance increasingly takes shape as an ‘infrastructural battle’,” which includes government actions, countermeasures by activists and users, and consequently, transformation of the media as a result of the aforementioned [6]. Various actors have been identified as the key actors invested in this process: the state itself, specific governors, or agencies such as Roskomnadzor (the federal executive authority that supervises information and communications technologies (ICT), data flows, and other protective and restrictive measures in the sphere of Internet regulation). Instances also vary, from restrictions on data storage outside Russia to restrictions on social networks.

Data storage became a key concern in Russia at roughly the same time that the General Data Protection Regulation (GDPR) legislation was introduced in the European Union. In Russia, it results in a series of measures, among them the “Yarovaya Laws” package (see the details further). Restrictions on online speech were equalized with laws governing public spaces (affecting online “spaces” such as social networking sites) and prohibited any humiliation of the state, national symbols, or the government (Claessen, 2020). Later, a package of legislation was introduced to provide a backup for critical infrastructure and information gathering about all traffic exchange points in Russia. Even as several of these laws were discussed and proposed to the State Duma, they were discussed as a “sovereign Internet law,” yet they consisted in a series of proposals for different laws. The deputies proposing one of these new laws, Klishas and Lugovoi, characterized them as protectionist: “we need protective measures to provide the long-standing and sustainable functioning of the Internet in Russia and to increase the stability of Russian Internet resources” (Law proposal number 608767-7) [7]. Indeed, the numerous legislative packages of the late 2010s impacted Internet infrastructure; among other consequences, they compelled Internet service providers to invest in costly technologies in order to backup data.

Russian practices of Internet governance have attracted the attention of multiple scholars, who have compared them to Chinese state measures (Deibert and Rohozinski, 2010), regarded them as claims to sovereignty (Nocetti, 2015), or even as attempts to “disconnect” Russia from the World Wide Web (Soldatov, 2019). Such explanations assume that the Russian state is the most important political actor that meaningfully contributes to shaping Internet policy in Russia. The major opposing actor is held to be the “public sphere” of the RuNet or oppositional newspapers (Sivetc, 2019). The RuNet is often used as a
synonym for the Internet in Russia itself, and yet this label corresponds rather to a language, a physical network — or set of networks — used to convey the notion of a “part” of cyberspace that is imbued with a sense of belonging and identity. The first publications to emphasize this meaning emerged in the early 2000s (Schmidt, et al., 2006). Later on, the same word was repeatedly used but endowed with different meanings — from the interactions of business associations and the IT sector to the politically-charged social and political movements. An example is Siniye Vederki, a movement opposing governors’ privileges to use the roads while ignoring the rules shared by other users, which we witness in a popular YouTube film directed by the Russian journalist Andrey Loshak (2019).

We would argue that the contemporary Internet in Russia escapes the bounds of this determination, one that is closely aligned with the Moscow-based public sphere. At the very least, we should consider its complex dynamics, given that over the years it has been influenced by several groups with different imaginaries (Asmolov and Kolozaridi, 2017). It is still driven by different vectors being a “runaway object” rather than a phenomenon with stable boundaries (Asmolov and Kolozaridi, 2020). It means that each group has its own understanding and imaginary of the technology and influences the Internet accordingly. This tendency, initiated by a particular group is what is called ‘vector’ here. Therefore, when dealing with ‘RuNet’ as a term, one should be sensitive to the context and attentive towards the particular understanding of the term by the actors who use it [8]. There are also plenty of local nets in Russia where people were never concerned with the ‘RuNet’ as a reference for their own projects.

Moreover, taking into account these different perspectives as to what the Internet is in Russia, we find that the “multistakeholderism” approach is complicated by the fact that the boundaries between stakeholders have been blurred from the Internet’s inception. Historically, the key stakeholders in the Russian Internet were individual pioneers and NGOs, organized in collaboration with the government, universities, international organizations, and, rarely, businesses (Kolozaridi, 2018). A case in point was the Russian Institute for Public Networks (RIPN, RosNIIROS in Russian), which was responsible for domain registration until 2001, and was both an initiative of civil society and the business sector. A contemporary example is the Agency for the Strategic Initiatives (ASI), which, while formally an NGO, was established by the Russian government (Rasporyajenije, 2011) [9]. None of these organizations can be clearly demarcated as “state,” “business,” or “NGO,” and only a few examples seek to uphold such a separation (e.g., Roskomsvoboda, a group of activists who keep their activities distinct from other sectors). Such “hybrids” co-exist with stakeholders with more temporarily and institutionally stable roles, so that big corporations — Mail.ru, Yandex, Kaspersky Lab, and GAFAM — operate alongside activists like Roskomsvoboda. This hybridity creates political difficulties for enacting classical multistakeholderism.

So far, the Russian case seems to present dissimilarities with respect to both the Western and Chinese contexts. Not all the stakeholders are clearly distinguishable, and the state was largely disinterested in strong Internet regulation until the 2010s. Yet the implications of this may vary. Whereas for the proponents of multistakeholderism as a universal governance model these dissimilarities are taken to be a deviation that can and should be overcome, for others such claims may raise suspicion for their underlying assumption that universal models of governance are actually possible and desirable.

The legacy of regulatory and research traditions

Many Internet researchers adopt approaches that derive from media studies and which, more specifically, pertain to the freedom of speech of the (oppositional) media. This appears to contribute to the path dependence of the RuNet as a key research theme, with RuNet having largely been described as an alternative public sphere (Schmidt, et al., 2006). In both public and popular narratives (Loshak, 2019; Soldatov and Borogan, 2015), RuNet stands for “the Internet in Russia” and has its origins in Russian emigrant communities in the West [10].

Turning to other aspects of this history, the picture appears somewhat different, as there were no restrictions placed on pirated content until 2013, no prohibition on unauthorized public Wi-Fi use, and no requirements to use the Russian language for non-Russian-speaking minorities [11]. However, these issues diverged from the media researchers’ agenda vis-à-vis the Russian Internet. Their focus has engaged issues of censorship,
disinformation, state propaganda, the public sphere in social networks, and similar subjects that forge a strong link between media studies’ objects of research and the political regime (Maréchal, 2017; Etling, et al., 2010; Oates, 2016).

Another important issue concerning path dependence is the comparison of Russia with other non-Western countries such as China. Yet the networks that constitute the Internet in Russia spread and appeared in different cities, often independently from each other and from the federal government. By contrast, Chinese networks were built by the government in a much more centralized fashion. Russia’s claims to Internet sovereignty are occasionally treated as exceptional and Russian-specific, despite the fact that following the Snowden case we have seen similar claims in other countries, as with Germany’s “digital territorialization” (Möllers, 2021) or Brazil’s initiatives to de-Americanize and de-globalize ICANN (Mueller and Wagner, 2014). The issue here is that the chosen focus of the aforementioned media studies research agenda may unwittingly contribute to an asymmetrical treatment of different countries’ Internet policies by epistemologically limiting studies of the “Internet in Russia” to questions of authoritarian control and the suppression of dissent rather than opening these questions to include other considerations for changes in Internet policy.

The final limit is an excessive Moscow-centrism, which often neglects the fact that Russia is a federation with contrasting infrastructures. Moreover, the USSR encouraged technical development and various faculties in universities prepared specialists in system engineering, computer sciences, math, cybernetic systems, and many other fields, all of which emerged in different periods (1960s and 1980s especially). Thus, in the 1990s, after the Soviet Union’s collapse, plenty of individuals were knowledgeable about computers and networks, notwithstanding the fact that they had only ever seen recent Western developments at annual exhibitions in Moscow. Some of these specialists emigrated from Russia, but others stayed and became Internet pioneers, and developers, or Internet service providers in the commercial and academic sectors. The Russian Internet has been shaped across many more regions, and by far more individuals, than a “Moscow-centric” approach can account for.

**Nets beyond RuNet: An alternative understanding of the “Internet in Russia”**

Internet development in Russia was not centralized but occurred independently in different cities. Contrary to some other countries, the absence of nationwide efforts at networking resulted in a plethora of local networking efforts (“nets”). This makes the urban level of analysis an important theoretical frame for understanding what the Internet is in Russia (Kolozaridi and Dovbysh, 2020). There have, therefore, been numerous self-described “nets,” and each presents its own “constellation of relations between different actors [...] and can include various elements that need to be distinguished empirically.” (Yuldashev, 2020)

Such nets were, in some instances, language- and imaginary-based; for example, Tatnet, a Tatarian Internet, has been strongly identified with the language and culture of the Tatars (Sibgatullin, 2008; Shchetwina, et al., 2019). Nets could also coincide with city borders and depend upon a specific infrastructure (e.g., Tonet, which originated in Tomsk; see Kolozaridi and Muravyov, 2020; Yuldashev, 2020). Not all networking initiatives in the early years of the Internet in Russia distinguished themselves as “nets,” but what was common to all was the absence of centralized projects of networking. This can be understood as an infrastructural legacy of the USSR, which lacked a successful centralized network project (Peters, 2016; Yuldashev, 2020).

This multiplicity of nets across Russia is still not a key theme for researchers of the Russian Internet, who concentrate on what has happened to the resources of what they call the RuNet and pay more attention to the contestation between civil society and the state. By including nets within this discussion and treating the RuNet as only one among others can reveal more angles, engaging global, national, and local scales. The Tonet has not been subject to government restrictions but became much less significant as a result of the increased traffic (and use as well) on mobile devices (due to “unlimited” tariff packages) and other aspects of the “triple revolution” (Rainie and Wellman, 2012). In such cases, we need to nuance the opposition of global vs. local, insofar the local may not imply the national state at all, as was also discussed in Duarte’s research on Indians. Sovereignty in the case of “nets” might include a claim to counter the hegemony of the
We should also consider the diversity of Internet infrastructure in Russia. In the islands of Kuril (Borodulina, 2018) or in Yakutia (Vasiliev, 2016), the Internet has been mostly mobile and therefore highly expensive. This is largely due to the year-round severe low temperatures and the presence of the sea, which have rendered the installation of landlines excessively complicated. However, this does not mean that islanders have not found ways to interact with the Internet [12]. They have developed ways to interconnect via WhatsApp, or have used a combination of online and off-line practices, such as exchanging movies via hard drives. Such examples demonstrate that infrastructure regulation will vary depending on material preconditions, as well as cultural practices and the local technosocial legacy. In other words, given infrastructural differences, which has its origins in the history of the Internet in Russia, federal level Internet policies may affect regions differently in practice.

The key implication of this brief overview for understanding Internet sovereignty in Russia is that the existence of a multiplicity of nets complicates equating the “Internet in Russia” with the actions and strategies of the ruling political regime in regulating the Internet. Despite the fact that federal laws are intended to be implemented all over the country, local peculiarities might challenge the way of these legislative initiatives when they are implemented.

First of all, we can consider the ideas of user sovereignty developing on the local level. Each Russian city and region (as well as a national republic), has its own program not only for access penetration but also digital literacy programs. Of course, it does not turn all the consumers into citizens automatically, but it is important to consider that users’ perspective might vary. Moreover, individual users and communities might implement their own initiatives, like mesh-networks, low-tech Internet (De Decker, et al., 2020). These initiatives can be combined with local networks that sometimes still survive in Russia, as the Internet penetration was not centralised and often started from a yard with several connected which are still connected. So far “nets” like Tatnet or Tonet together with these user-centered nets can become a ground for political imagination of other types of sovereignty while not upholding the strict opposition between the state Internet sovereignty and global governmentality.

These nets could be a way of enacting “network sovereignty” (Duarte, 2017); one that is based not on the state’s self-determination in Internet governance, but rather places an emphasis on the local conditions that contingently shape the formation of a given net. Their inactivity means that until now “nets” (except for Tatnet) have not been mobilized by any political or social movement, however this does not mean that it could not happen in future.

---

**Reassembling sovereignty and the Internet?**

This section offers a reconsideration of Russian Internet sovereignty claims in light of the aforementioned historical discussion. We believe that some of the discussions on Internet sovereignty have been subjected to “the descriptive fallacy” (Krasner, 1999) — an idea that sovereignty corresponds to something in reality. But rather than attempting to re-define sovereignty so that it finds something it can correspond to, we propose instead to follow Werner and de Wilde (2001), who have argued that sovereignty claims can be more productively understood as a form of a speech act. In this vein, studying sovereignty claims is an attempt to understand why a given actor decides to rhetorically “enact” its independence. With this argument, we do not suggest that these speech acts do not have material and infrastructural consequences. Yet we shift the focus towards the ways in which sovereignty claims help actors to linguistically perform ideas of autonomy and independence. In the context of global Internet governance, this means to question and consider the conditions that prompt such sovereignty claims by states and other actors. Couture and Toupin (2019) have used this approach to argue that sovereignty claims are made to counter hegemonic tendencies in the broadly conceived politics of digital technologies, which explains why discourses on Internet sovereignty are largely
In Russia’s case, we propose that it can be fruitful to associate the use of “sovereignty” in both the aforementioned “sovereign RuNet” and in “sovereign democracy.” This latter is a concept most notably developed by the former head of the presidential administration and ideologue Vladislav Surkov in 2006. This comparison has been previously discussed, especially in the late 2000s (Asmolov, 2010). The key claim has drawn on the idea that Internet sovereignty claims become a kind of “creation of [a] national cyberzone” (Asmolov, 2010).

Surkov’s coinage, sovereign democracy, was intended to advance an understanding of democracy that would be compatible both with global understandings of democracy and a national interpretation of the process of governance, involving the primacy of national over international institutions. This idea has often been interpreted as an attempt to mask non-democratic rule using the guise of a novel democratic label, all the while hollowing out the institutions and practices of contemporary “liberal democracies.”

While this may be true, we propose that it can be also productive to approach the question differently. Morozov argues that this conception of sovereign democracy should be approached assuming “neither full sincerity on the part of high-ranking ideologues nor pure contingency of the discursive articulations they are trying to establish” [13]. Wielding a post-structuralist theoretical framework, Morozov asserts that the liberal universalist perspective construes Russian elites’ claim to sovereignty as “reactionary in the sense that it means moving back in historical time from post-modernity into the modern world” [14].

This interpretation allows us to see that “sovereign democracy” expresses the tension between democracy’s universal character and its Western incarnations. Consequently, sovereignty claims are performative in their rhetorical constitution of a counter-hegemonic discourse to the West’s liberal and universalizing project, of which “the global Internet” forms a part. Discussions on Internet sovereignty in the context of Russia and other countries can thus be reframed if they are considered in light of the hegemonic power relations that structurally underpin Internet governance.

This is largely because the field of Internet governance is inseparable from Western liberal hegemony and its attendant power asymmetries. As Ali (2018) has demonstrated, the Internet has never been fully “decentralized,” in the sense that the Internet has reproduced colonial hierarchies across infrastructure, technology, discourse, and governance models (see also Mathew, 2016). Relating to issues of Internet sovereignty, Ali criticizes Mueller’s formulation of the problem of alignment for its neglect of how the Westphalian system has evolved through the modern, colonial world system. Although a discussion of the relationship between Russia and colonialism/coloniality extends beyond the scope of this paper, we would venture to argue that Russian elites’ Internet sovereignty claims can be construed as a “rebellion” against Western-centric “global” Internet governance (see Tlostanova [2015, 2012] on the relationship between coloniality and the post-Soviet space).

In this sense, the “sovereign Internet” is not reducible to an authoritarian policy, aimed at “disconnecting from the global Internet.” Instead, it can be understood as an articulation of tensions, conditioned by the power asymmetries of global (Internet) governance. This analysis reveals that the counter-hegemonic tendencies of various actors can be attributed to the unequal distribution of power within contemporary Internet governance frameworks.

**Internet policy at the crossroads of statecraft and political regimes**

In our attempt to contextualize Russia’s Internet policy, our characterization of Internet governance frameworks allows us to consider policy changes as more than state-led efforts at the prolongation of an authoritarian or hybrid political regime. Instead, this interpretation calls for more careful analytical attention in distinguishing between regime-centered explanations and those that tie together statecraft, sovereignty, and the Internet (e.g., Möllers, 2021; Budnitsky, 2020).

Moreover, regime-centered explanations of the dynamics of Russian Internet policy occasionally build on a
problematic exoticization of the country’s political history. For example, it feeds into a narrative that the goal of Russian Internet policy is simply “the accumulation of power and wealth for Russia’s kleptocratic elites” [15] and unproblematically asserts that the “media in Russia have always served as instruments of political propaganda, going back to the country’s first newspaper” [16], or that the “Russian Net built upon the cultural tradition of personal blat networks” [17], implying that the informal quality of RuNet is based on corrupted networks rather than grassroots movements.

This perspective extends a history of exoticization and an othering of Russia by the West, dating back to, at the very least, the Cold War era (Bonnett, 2004, 2002) [18]. While this comparison may appear to be far-fetched to some, similar readings of contemporary Internet governance exist, which refer to current policy dynamics as “the digital Cold War” (Mueller, 2013; discussed in Ali, 2018). What adds an additional level of complexity is that Russia as well as other post-Soviet countries cannot be that easily fitted within the Global North/South distinction; some scholars suggest speaking of “Global East” to theorize the particularity of the post-Soviet condition (Müller, 2020). The explicitly political need for autocratic survival may indeed be at the root of recent Russian Internet policy, as exemplified in the legislation that followed the Bolotnaya protests of 2011–2012 (protests in response to the flawed elections to the State Duma [Tselikov, 2014]). However, other legislative initiatives — including “Internetization” or “informatization” infrastructural programs — were adopted much earlier.

Some of these legislative initiatives began during Dmitry Medvedev’s tenure as prime minister and, later, as president. They were aimed at extending Internet access to all cities, towns, and villages, as well as to schools, universities, and colleges. Later, these initiatives expanded to include e-government, decreasing taxes on IT companies, and the provision of Internet connection for public-private services, including hospitals and the postal service. Some of these initiatives were framed as Medvedev’s policy of “modernization” (Medvedev, 2009; Kremlin.ru, 2011) [19]. Within this discourse, modernization is the attempt to comprehend the Internet and digital technologies as a continuation of modern statehood, in similar fashion to electricity (electrification) or, more broadly, to industry (industrialization). This framing resonates with projects in which socio-technical systems were supported or initiated by the state (Edwards, 2002). They might not fully overlap with “modernization” as a term in scholarly research, yet they were framed in a similar way, albeit using IT instead of trains and electricity. Conception(s) of Internet sovereignty can challenge the discourse of modernization and may invite an altogether different framing (Floridi, 2020). The installation of other infrastructures, such as electricity grids, have often been led by state actors as part of national modernization efforts; by contrast, the Internet has, in many contexts, evolved into an infrastructure that poses a challenge to the state and therefore elicits attempts to domesticate it.

This returns us to the definition of the state as a modern entity with modern institutions, which has in some ways to tackle the challenges posed by the Internet to its modernity.

This requires a nuanced approach as well, given that the Internet in the 2000s might have encompassed other imaginaries, both within global institutions (Mansell, 2012) and at the national level. This period in Internet history preceded the Snowden revelations, debates surrounding online fake news, the controversy over Cambridge Analytica, online mobilization during the Arab Spring, and so forth. In the Anglophone context, moreover, the dotcom crisis loomed larger than in the post-Soviet countries. From this perspective, Russia appears to be closer to the countries of the Global South. Here, sovereignty claims can be understood as a reaction to changes in both Internet and Western politics.

However, we do not wish to suggest that political regime has no influence on Internet policy whatsoever. Rather, we would like to draw attention to other possible explanations that have previously been given less scholarly attention. For instance, as we have previously argued, Internet policy changes after Bolotnaya protests can be seen as caused by the rationale of political regime, while Medvedev’s policies can be better comprehended as a continuation of statecraft.

Consequently, we argue that the framing of Internet sovereignty-related policies exclusively as a means of advancing the agenda of “networked authoritarianism” blinds analyses to the broader context of Internet governance, in which states may employ a variety of both technical and non-technical means to craft a
Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case

The (inter)national shaping of Internet policy

A further perspective that supports our argument here pertains to the ways in which Internet policy is shaped by both domestic and international factors (DeNardis, 2014). For instance, in Russia, several competing explanations have been given to account for the changing landscape of the state’s Internet policy. In the global policy arena, it has been argued that for Russia, regulation of information space is tightly connected to state sovereignty and can be dated back to Russia’s proposed UN resolution in 1998 (Kovaleva, 2018). Moreover, as Claessen (2020) has argued, the logic of securitization in Russian Internet policy has also been influenced by the Snowden revelations, creating “a break in Russia’s style of regulation and control.” Overall, Claessen [20] claims that recent tendencies in Russia’s Internet policy towards a centralization of control over Internet infrastructure can be explained by its “stance on the primacy of the state in international Internet governance.”

Alongside this research, which traces Russia’s stance on Internet sovereignty across various issues (including data localization or information security in the global policy landscape), other lines of scholarship, noted above, have emphasized internal political dynamics as an explanatory factor.

Here, it is important to take stock of the Internet’s divergent scales and components, which we introduced above, and which are transnational, global, national, and local, and cannot be construed as binary opposites. Each involves different aspects of regulation; thus, even as it regulates infrastructure within national borders, the state might not ever attempt to regulate the global communication network. Yet insofar as these scales are entangled, interventions do, to an extent, implicate “all” the Internet as a matter of concern.

Further research is needed to conceptually disentangle the interconnection of scales — global and local, transnational, and national — that contribute to specific Internet policy developments. Without such analytic disentanglement, we may fall into a simplistic understanding of the dynamics of Internet policy in two respects. We may grasp them as a way in which the government tightens its control over the Internet control in order to further consolidate a political regime, or see them as a continuation of the territorialization projects characteristic of the modern state per se, regardless of the nature of its political regime.

Instead, a more nuanced approach to comprehending Internet sovereignty would attempt to disentangle the influence of a given regime from the continuation of the statecraft project more broadly. An analysis of a given Internet policy, moreover, should account for global influences, such as the Snowden revelations, as well as for the factors tied to the national political regime, including Internet shutdowns and Internet censorship to suppress dissent. In Russia, we believe that such an approach is much needed. Current portrayals of Russia’s Internet policy, in both scholarly and public discussions, and both domestically and abroad, continue to confer an excessive prevalence to the influence of its political regime.

Conclusion: Broadening research focus in studies of Internet governance

In this article, we have considered prevalent ways of thinking about Internet sovereignty and have proposed alternative points for analytical focus, drawing upon a theoretical analysis and historical analysis of the Internet in Russia. Our key aim has been to reconstruct the discussions of different concepts surrounding “Internet sovereignty” and to suggest how these discussions can be approached differently. Specifically, we have drawn attention to how distinctions between global, local, transnational, and national scales, as well as statecraft and the agency of specific political regimes, can complicate existing portrayals of Russia’s evolving Internet policy.

We began with an analysis of ongoing discussions about the Internet and sovereignty. Our claim here is that the Internet can be understood not only as a global cyberspace, but rather — following existing scholarship at
the intersection of STS and Internet governance — as a set of infrastructures, which are both sites where, and tools by which governance and regulation are exercised and coordinated.

Later, we proceeded to assess recent and earlier scholarly work, which has attempted to explain and understand Internet sovereignty in the Russian context. We have identified what we believe to be the shortcomings of their prevailing research focus; an excessive focus on Russia’s capital city as a locus of Internet power and the controversies that surround it (which we have termed “Moscow-centrism”); a collapse of the distinctions between the agenda of a given political regime and the prolongation of statecraft; a lack of attention to other “nets” beyond RuNet; narrowly national explanations, or, in other cases, a problematic analogization with China and other countries with similar political regimes, but often diverging policies. In the case of Russia, authoritarian tendencies have shaped the state’s practices, among others, of control and censorship though the political regime itself cannot serve as an exclusive explanation for these changes.

In our thinking about Internet sovereignty as a concept, we propose an interpretation of sovereignty claims as performance, rhetorical acts whose primary function is to counter hegemonic tendencies. In Russia, this implies that sovereignty claims are both a reaction to Western-centered Internet governance frameworks, and a reaction to the technology that compels the state to act as a modern state. Both explanations appeal to processes of statecraft, rather than to the results of a particular political regime’s policies. To clarify, we do not intend to claim that the political regime plays no role whatsoever in shaping Internet policy; instead, we argue that researchers should be more reflexive as to which changes can be attributed to a given political regime, and which cannot.

We propose that, in their framing of historical continuities and divergences, future discussions of Internet sovereignty may greatly benefit from an elaboration of two critical distinctions. First, a disentangling of the interconnection of scales (global and local, transnational and national) that shape a particular Internet policy. Second, a distinction between the influence of a political regime from continuations of statecraft in the domain of Internet policy.

Lastly, we call for more considered and thoughtful choices in researchers’ processes of constructing a particular historical continuity. The reason for this is that such choices may either narrowly focus upon, or otherwise eclipse, specific government actions and events, thereby distorting the analytical outcome. As we have tried to demonstrate, taking into account the plurality of nets in the evolution of the Russian Internet, or analyzing Medvedev’s modernization project, reframes discussions surrounding Internet sovereignty. Our proposal for further research is to emphasize the inclusion, not exclusion, of diverse case studies in order to epistemologically reframe the field of Internet governance research.

In recent years, the public discussions on digital sovereignty have largely contributed to discursively shaping an opposition between authoritarian and democratic conditioning of the Internet’s future. While we do not suggest abandoning discussions about the influence of political regimes, we believe that the excessive focus on such binary opposition limits the possibilities of political imagination that potentially can go beyond this dichotomy, both in academic research and public debates. We see our article as a call for such imaginative ventures.

About the authors

Polina Kolozaridi is a social researcher focusing on the Internet. She coordinates a grassroots community of researchers called the Club for Internet and Society Enthusiasts (клуб любителей интернета и общества, http://clubforinternet.net/). She holds courses about Internet studies and critical data studies at the Higher School of Economics. E-mail: poli [dot] kolozaridi [at] gmail [dot] com

Dmitry Muravyov is a Visiting Scholar in the School of Politics and Governance, Faculty of Social Science at Higher School of Economics and a member of the Club for Internet and Society Enthusiasts (клуб
E-mail: dvmuravyov [at] gmail [dot] com

Notes

1. For example, Natalia Konradova (2020) has studied RuNet users as a community of repatriates and residents in big Russian cities, who first connected in the 1990s and are frequently associated with the early years of the Russian Internet.


8. For example, there is a tradition of treating RuNet as an IT-sphere and business-centered phenomena (see the annual event The economics of RuNet or Andrey Tselikov [2014]). In contrast activists claim it to be the free space for people’s initiatives (like Roskomsvoboda and the Internet Protection Society [https://www.ozi-ru.org]).


10. However, why we should consider “the West” to be monolithic is also a question that could be raised.

11. It is worth noting that there were not many initiatives in relation to online representation and the provision of technological support to this end, e.g., keyboards for “minor” languages. These issues have not, however, been a focus of interest for Anglophone researchers.

12. Interestingly, here we meet another narrative about the right to Internet access. In the cases we refer to, all users do have access. The network, however, might be not as efficient as 5G or a landline connection.


18. We can trace the lineage of the division between Western (and later, “global”) and Soviet subjects back to the historical rifts between liberal and Stalinist subjects (Krylova, 2000). This lineage can inform an understanding of contemporary narratives about the Russian regime as a legacy of the previous epoch, anchored in the liberal oppositional identities that emerged during the USSR. We also acknowledge that
historians and anthropologists try to challenge this exoticisation, but remark that their work remains largely independent from core discussions about Internet governance.


References


Eva Claessen, 2020. “Reshaping the Internet — The impact of the securitisation of Internet infrastructure on


Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case


Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case


doi: [http://dx.doi.org/10.17645/mac.v5i1.808](http://dx.doi.org/10.17645/mac.v5i1.808), accessed 9 April 2021.


doi: [https://doi.org/10.7551/mitpress/9780262014595.001.0001](https://doi.org/10.7551/mitpress/9780262014595.001.0001), accessed 9 April 2021.


doi: [https://doi.org/10.1057/9781137483591](https://doi.org/10.1057/9781137483591), accessed 9 April 2021.


Ainur Sibgatullin, 2008. *Татарский Интернет (Tatarski Internet or Tatar Internet)*. Нижний Новгород (Nizhny Novgorod): Медина (Medina).


Andrei Soldatov and Irina Borogan, 2015. *The red Web: The struggle between Russia’s digital dictators and( לו歌词)


**Documents**


**Editorial history**

Received 2 April 2021; accepted 7 April 2021.
Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case

by Polina Kolozaridi and Dmitry Muravyov.

First Monday, volume 26, number 5 (May 2021).

doi: https://dx.doi.org/10.5210/fm.v26i5.11687