Selected Papers of #AoIR2021:
The 22nd Annual Conference of the
Association of Internet Researchers
Virtual Event / 13-16 Oct 2021

TOWARDS AN INFRASTRUCTURE-BASED SOCIOLOGY OF DIGITAL SOVEREIGNTY PRACTICES: THE "PILOT CASE" OF RUSSIA

Francesca Musiani
Centre for Internet and Society, French National Centre for Scientific Research (CNRS)

Digital sovereignty as infrastructure-embedded "situated practices"

Today, a number of high-profile initiatives across the globe (including the Digital Services Act in Europe, the "Great Firewall" of China, Russia's "sovereign Internet" and "anti-Apple" laws, and many others) are concrete implementations of the "digital sovereignty" principle: i.e. the idea that states should "reaffirm" their authority over the Internet and 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 largely neglected. In this proposal, I argue that the concept of (digital) sovereignty should also 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 this contribution is also a call for a wider and comparative research programme, I will focus here on the "pilot case" of Russia, which is the subject of an ongoing research project.

This contribution draws primarily upon three lineages of literature. The first lineage includes Internet governance (IG) studies and in particular its subset that addresses the concept of digital sovereignty and the relationship between digital networks and states (Mueller, 2010, 2020; Haggart et al., 2021; Budnitsky & Jia, 2018; Couture & Toupin, 2019; Pohle & Thiel, 2020). The second lineage encompasses studies of information systems according to science and technology studies (STS) and more specifically

Suggested Citation (APA): Musiani, Francesca. (2021, October). *Towards an Infrastructure-based Sociology of Digital Sovereignty Practices: The "Pilot Case" of Russia*. Paper presented at AoIR 2021: The 22nd Annual Conference of the Association of Internet Researchers. Virtual Event: AoIR. Retrieved from http://spir.aoir.org.

infrastructure studies (Bowker and Star, 1999; Galloway, 2004; DeNardis, 2009; Barry, 2006; Easterling, 2014; Karasti & Blomberg, 2018). The third, more recent, lineage seeks to combine the lenses of infrastructure studies and IG studies (e.g. Epstein et al., 2016; Musiani et al., 2016; DeNardis, 2009).

Russia, a "pilot case" for an infrastructure-based sociology of digital sovereignty

In several respects, the Russian Federation, with its "national" Internet (Runet), is an interesting "pilot case" to work towards an infrastructure-based sociology of digital sovereignty. In the first decade of the 21st century, the technical constraints on the construction of the Runet have remained mostly invisible to its users (Deibert and Rohozinski, 2010). However, since the early 2010s, increasingly strict regulations imposed by the government have made these aspects more evident (Soldatov and Borogan, 2015); in particular, Roskomnadzor, the federal government communications control body, has seen its jurisdiction and reach rapidly extended, and relies on an important nexus of collaborations with other public and private actors. Russian authorities actively move towards an autonomisation and "sovereignisation" of the RuNet through the adoption of new laws to counter foreign influences and agents, as well as their devices and applications (FIDH, 2018).

The team of the *ResisTIC (Criticism and circumvention of digital borders in Russia)*[1] project analyzes how different actors of the Runet resist and adapt to the recent wave of authoritarian and centralizing regulations. The project has a focus on online resistance and the lesser-known social practices and techniques deployed for circumventing online constraints, focusing on the technical devices and assets involved in surveillance and censorship, and on the strategies of resistance and circumvention 'by infrastructure' that follow. Indeed, in response to the Russian government's increasingly authoritarian grip, direct political confrontation is difficult and risky; thus, the use of infrastructure is a way to indirectly bypass constraints and coercion. A number of dynamic behaviors, which can be qualified as infrastructure-based ruse and resistance, have emerged in close response to legislation. Russian "digital resisters" adapt to new laws and invent new techno-legal tweaks that challenge the Russian lawmaker.

In its final part, this contribution outlines four main dynamics identified by the ResisTIC project in relation to digital sovereignty as a set of infrastructure-embedded practices (see also Daucé and Musiani, 2021). First, the Russian government raises a number of obstacles against foreign techniques and alternative infrastructures, considered as "subversive". Second, the technical implementation of these infrastructure-based coercive measures often results in "collateral damage". Third, the current Runet context leads to the creation and development of new "digital champions" under an increasingly close government supervision, such as the pressures and manipulations exerted by the State on particular platforms and their algorithms. Finally, critiques of "governance by infrastructure" dynamics emerge among internet users, which contributes to the rise of new forms of "resistance by infrastructure". Ultimately, the analysis of these dynamics

[1]Supported by the French National Research Agency (ANR); https://www.resistic.fr.

shows how the Russian discourse on Internet sovereignty as a centralized and top-down apparatus paradoxically open up technical and legal opportunities for mundane resistances and the existence of "parallel" Runets, where particular instantiations of informational freedom are still possible.

References

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

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

Budnitsky, S. & Jia, L. (2018). "Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance", *European Journal of Cultural Studies*, 21, 594–613.

Couture, S. & Toupin, S. (2019). "What does the notion of "sovereignty" mean when referring to the digital?", *New Media & Society*, 21, 18.

Daucé, F. & Musiani, F. (eds., forthcoming 2021). *Infrastructure-Embedded Control, Circumvention and Sovereignty in the Russian Internet*. First Monday, special issue, May 2021.

Deibert, R. and Rohozinski, R. (2010). "Control and Subversion in Russian Cyberspace", In Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain (eds.), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge, MA: MIT Press, pp. 15-34.

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

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

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

FIDH (International Federation for Human Rights, 2018). *2012-2018: 50 New Laws to Ban Freedom of Expression in Russia*.

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

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

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

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

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

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

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