Selected Papers of #AoIR2025:
The 26th Annual Conference of the
Association of Internet Researchers
Niterói, Brazil / 15 – 18 Oct 2025

RUSSIAN INTERNET INFRASTRUCTURE IN THE AGE OF DIGITAL SOVEREIGNTY AND INFRASTRUCTURAL COERCION: THE CASE OF TSPU

Dmitry Kuznetsov
University of Amsterdam

Introduction

The landscape of internet governance is no longer guided by a singular view of global connectivity. Increasingly, states promote multilateral internet governance (Mueller, 2017) discussed in terms of digital or cyber-sovereignty (Stadnik, 2021; Hong & Goodnight, 2019), often exemplified by Russia and the PRC (Epifanova, 2023). When viewed through the lens of infrastructural ideology, these states differ substantially in the development and evolution of network and information controls, and understanding their particular arrangements requires dedicated case studies. Focusing on Russia, this research aims to explore how the Russian state attempts to overcome infrastructural and institutional inertia to impose coercive controls over its informational landscape. Using the rapid deployment of Technical Measures to Combat Threats (TSPU) as a case study, this paper focuses on the role that industry actors play in negotiating or resisting infrastructural coercion.

Concepts and Context

Maxigas and ten Oever (2023) define infrastructural ideologies through hegemony: the use of power to establish and maintain a taken-for-granted social order in pursuit of a “particular purpose” (p. 284). Crucially, they highlight that one may evaluate “the performance of a hegemonic project” (p. 273) by whether the ruler has to rely on coercion. Developing this framework, this paper introduces infrastructural coercion as a means of crisis-driven redefinition of socio-technical arrangements. Unlike hegemony, which relies on tacit acceptance, infrastructural coercion operates through explicit, accelerated interventions to reshape technological systems and compel compliance, sidestepping previous concerns such as financial costs or social resistance.

I argue that following the full-scale invasion of Ukraine, the commonly accepted set of principles that governed Russia’s media and ICT spheres lost relevance. Before March 2022, the state did not rely primarily or exclusively on direct censorship or coercion, maintaining an environment of high uncertainty that promoted self-censorship and encouraged actors to ‘get it right’ on their own (Schimpfössl & Yablokov, 2020). In internet infrastructure, this was exemplified by the state’s use of decentralised control

Suggested Citation (APA): Kuznetsov, D.. (2025, October). *Russian Internet Infrastructure In The Age Of Digital Sovereignty And Infrastructural Coercion: The Case Of Tspu*. Paper presented at AoIR2025: The 26th Annual Conference of the Association of Internet Researchers. Niterói, Brazil: AoIR. Retrieved from http://spir.aoir.org.

over networks (Ramesh et al., 2020), offloading implementation costs and details of censorship to Internet Service Providers and Network Operators.
After March 2022, the regime has increasingly resorted to direct censorship, indicative of its “failure to impose a doxa” on society (Zeveleva, 2020, p. 28). I argue that the actions of the Russian state vis-a-vis both the content and infrastructure of the Internet can be viewed through the lens of infrastructural coercion: the explicit use of power meant to accelerate institutionalisation of new rules of the game. A notable example is the rapid and pervasive deployment of TSPU (Technical Measures to Combat Threats) measures: a hardware and software package that allows for centralised information control through use of Deep Packet Inspection (Xue et al., 2022).

Researching TSPU

The use of TSPU and DPI as a means of information control was first formalised in the 2019 amendments commonly known as the “Russian Sovereign Internet Law” (Stadnik, 2021), and then tested to throttle Twitter traffic in 2021 (Xue, 2021). At the time, commentators doubted the ambitious plan for total coverage, citing reasons such as lack of technical capacity, potential impact on quality of service, the “sensibility” of filtering all traffic, and the costs involved, as well as the potential for public discontent (Stadnik, 2021). The full-scale invasion of Ukraine required and enabled the establishment of a new hegemony among the key actors of the country’s ICT sector through coercion. This paper argues that the previously salient concerns had been relegated to the background, with wartime centralisation of information control justifying the substantial financial resources required for full deployment of TSPU and the subsequent transformation of Russia’s previously open ICT environment. To understand the trajectory of the development of Russia’s information infrastructure and systems of control, it is important to place them within their historical context, recognising the apparent shift towards domestic infrastructural coercion, and to consider how resistance activities have evolved. Therefore, this research approaches the subject through:

1. Collection and examination of relevant policies, such as the ‘sovereign internet’ law (FZ-90), the Yarovaya Law, and more recent amendments or implementation guidelines.

2. Tracing activities of key actors like the Ministry of Digital Transformation, Roskomnadzor, vendors of DPI solutions, ISPs, and the expert public who previously resisted state interference (Ermoshina & Musiani, 2021).

Using a discourse-historical approach (Reisigl & Wodak, 2016), this study combines analysis of legislative texts with an examination of publicly available sessions from the Conference of Russian Telecom Operators and Data Centres (KPOC) (2018–2024). KROS serves as a critical site for observing both administrative and infrastructural actors’ discursive and material negotiations, with sessions coded for recurring themes (e.g., compliance strategies, sanctions impact) and shifts in rhetorical framing over time.

Findings & Discussion

KROS discussions reveal operators' strategies for complying with Russian internet regulations. Operators often seek ways to minimise the impact of regulations like the

"Yarovaya" law on their businesses, including exploring legal loopholes such as changing licenses or using outsourcing. They also look for technical solutions to meet regulatory requirements, such as implementing DPI systems and traffic management technologies.
Furthermore, the analysis reveals the impact of Western sanctions on the Russian telecom industry. The need to replace foreign equipment and technologies has led to increased demand for domestic solutions. KROS presentations showcase Russian vendors developing and offering equipment and services to meet this demand, although challenges remain in achieving full import substitution.

I note that discussions of the forum shifted from ridiculing the various laws mentioned above to cautious calls for optimism for the post-invasion status quo. If in 2018 speakers openly mocked the ‘sovereign internet’ law and suggested ways to limit its scope, participants in 2024 carefully discuss the impact of the war, new bylaws and sanctions as temporary difficulties in an otherwise optimistic developmental trajectory.

This research contributes to the growing body of literature on the Russian post-war media and communication environment. The focus on KROS advances scholarship on internet governance by analysing implementers—not just policymakers or users—as critical agents in infrastructural transformation. By centring infrastructural actors, this research challenges state-centric narratives of digital sovereignty. It reiterates how technological tools like DPI are not neutral: their adoption reflects and reinforces ideological priorities such as the need for wartime centralisation and distrust of global interoperability, while their material limitations create sites of friction for state control, requiring substantial monetary investment and administrative effort.

Understanding ongoing transformations in Russia has implications for contexts with similar infrastructural arrangements. Russia’s case demonstrates that infrastructural coercion can rapidly transform decentralised systems into centralised regimes using globally available tools (e.g., DPI). This challenges assumptions that ‘great firewalls’ require unique institutional contexts (e.g., China’s) and raises urgent questions about the adoption of ‘neutral’ surveillance technologies in liberal democracies (Fuchs, 2013).

References

Ermoshina, K., & Musiani, F. (2021). The Telegram ban: How censorship “made in Russia” faces a global Internet. First Monday. https://doi.org/10.5210/fm.v26i5.11704
Epifanova, A. (2020). Deciphering Russia’s “Sovereign Internet Law”: Tightening Control and Accelerating the Splinternet (Vol. 2). Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V.
Epifanova, A. (2023). Tech Sanctions Against Russia: Turning the West’s Assumptions Into Lessons (Vol. 3). Forschungsinstitut der Deutschen Gesellschaft für Auswärtige Politik e.V.
Fuchs, C. (2013). Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance. Information, Communication & Society, 16(8), 1328–1359. https://doi.org/10.1080/1369118X.2013.770544
Maxigas, & Ten Oever, N. (2023). Geopolitics in the infrastructural ideology of 5G. Global Media and China, 8(3), 271–288. https://doi.org/10.1177/20594364231193950

Ramesh, R., Raman, R. S., Bernhard, M., Ongkowijaya, V., Evdokimov, L., Edmundson, A., Sprecher, S., Ikram, M., & Ensafi, R. (2020). Decentralized control: Network and Distributed Systems Security Symposium 2020. Proceedings, 2020 Network and Distributed System Security Symposium, 1–18. https://doi.org/10.14722/ndss.2020.23098

Reisigl, M., & Wodak, R. (2016). The discourse-historical approach (DHA). In R. Wodak & M. Meyer (Eds.), Methods of critical discourse studies (3rd edition). SAGE.

Schimpfössl, E., & Yablokov, I. (2020). Post-socialist self-censorship: Russia, Hungary and Latvia. European Journal of Communication, 35(1), 29–45. https://doi.org/10.1177/0267323119897797

Stadnik, I. (2021). Control by infrastructure: Political ambitions meet technical implementations in RuNet. First Monday. https://doi.org/10.5210/fm.v26i5.11693 ten Oever, N. (2021). The metagovernance of internet governance. In B. Haggart, N. Tusikov, & J. A. Scholte (Eds.), Power and authority in Internet governance: Return of the state? Routledge.

Xue, D., Mixon-Baca, B., ValdikSS, Ablove, A., Kujath, B., Crandall, J. R., & Ensafi, R. (2022). TSPU: Russia's decentralized censorship system. Proceedings of the 22nd ACM Internet Measurement Conference, 179–194. https://doi.org/10.1145/3517745.3561461

Xue, D., Ramesh, R., S, V. S., Evdokimov, L., Viktorov, A., Jain, A., Wustrow, E., Basso, S., & Ensafi, R. (2021). Throttling Twitter: An emerging censorship technique in Russia. Proceedings of the 21st ACM Internet Measurement Conference, 435–443. https://doi.org/10.1145/3487552.3487858

Zeveleva, O. (2020). Towards a Bourdieusian sociology of self-censorship: What we can learn from journalists adapting to rapid political change in Crimea after 2014. European Journal of Communication, 35(1), 46–59. https://doi.org/10.1177/0267323119897798