

Teplitsa | September 2022 – March 2023

# Disconnect and Conquer

## The Future of Censorship in Russia: Horizon Scanning Approach

[te-st.org](http://te-st.org)

# About the report

In this brief report, the authors look at how censorship in Russia might develop in the next few years: the main driving forces, trends and turning points. The report provides insight into where Internet censorship could strike next, how its effects could affect different segments of society, and, of course, what should be taken into account when planning methods to combat censorship. This research is an interpretation of joint work by Russian cybercensorship and civil society experts using the Horizon Scanning Method.

Horizon Scanning is a method of predictive analysis that takes into account a wide range of sources and indicators in order to identify trends that could lead to significant transformation in the world around us. Particular attention is paid to "turning points" with a strong and unpredictable influence on the development of certain processes. During the discussions, the participants were able to identify not only the trends that many experts can see, but also the so-called "weak signals". Weak signals are peripheral information, which is far away from the centers of attention and topical discussions.

This report was created by the Teplitsa. Technologies for Social Good (<https://te-st.org>). Teplitsa is a civil society capacity building project that aims to strengthen Russian civil society with the smart use of technology.

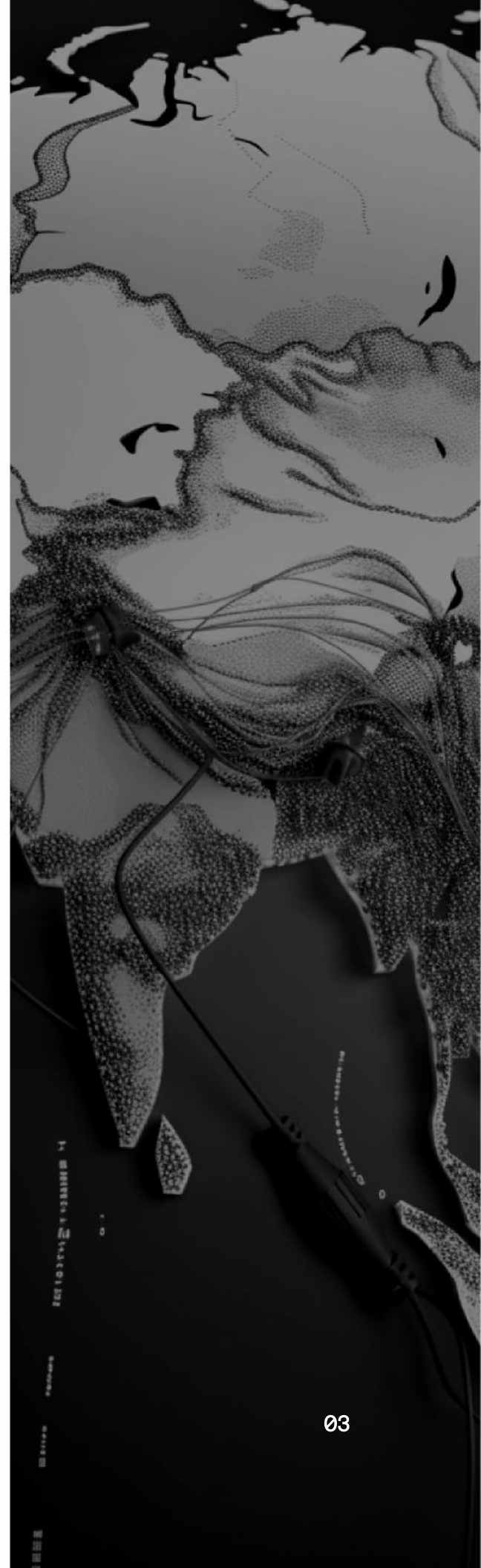
This report was originally produced in Russian and translated with the help of DeepL AI-powered translation tool into English, and edited by a group of volunteers.



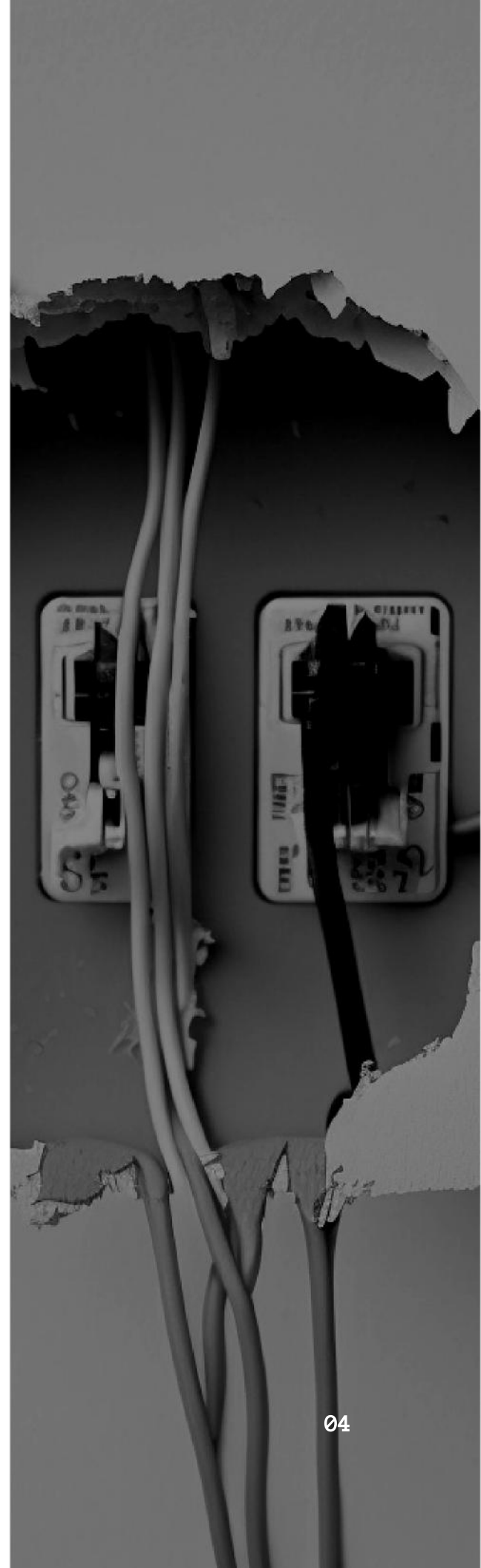
# Executive Summary

The report identified 19 trends of censorship development, 4 hypothetical events that can significantly change the state of censorship now (turning points), and 5 weak signals of the coming changes.

- The most important observed trend is the **creation of a substitute infrastructure in order to complete the process of isolating the Russian segment of the Internet** from the rest of the world. If Russia succeeds in both establishing blocking capabilities and will build its own stack of Internet infrastructure, then in possible cooperation with Iran and China – it might implement the "Splinternet" scenario, in which the global Web is irrevocably divided into large regional segments, where the information flows between which are significantly limited.
- **Isolation of Runet** (also often used the term "Pupation") – involves the deployment of technical infrastructure for effective blocking and moving the storage and processing of essential (and eventually all) information (payments, information exchange between state authorities, etc.) inside Russia, in order to shut down global services or even individual regions at any time without harming critical communications within the country.
- Preparation for the "Splinternet" scenario involves the creation of **duplicating international YouTube services, app stores, 0-to-0 infrastructure (online to offline)**, gaming and streaming platforms, messengers, search engines, browsers – in general, the entire stack of modern digital life.



- Authors agree that the Russians' perpetuation of the RuNet with the future prospect of a "Splinternet" may seem too ambitious a task, but the Russian state has both the motive and the means to carry it out so far. Experts agree that the isolation of the Russian Internet will happen in parts, but key elements are planned to be completed by the presidential election in 2024.
- Positive global trends that could affect censorship in Russia include the development of satellite Internet – as well as new technologies used in some cell phones that can communicate directly with a satellite. Researchers do not rule out the criminalization of ownership of such technology, as well as the "star wars" scenario and the militarization of orbit.





# Report Methodology

All Russians face censorship in Russia, regardless of which side of the Russian border they are on. As in other authoritarian regimes, the rise of censorship in the media and then on the Internet is one of the root processes that has permeated the entire period of Vladimir Putin and his protégé, Dmitry Medvedev. Since February 24, 2022, censorship has become avalanche-like. It is logical to assume that the regime will continue to seek ways to suppress freedom of speech, including technical, economic, administrative, and coercive means, not only inside the country, but also outside it, especially in the centers of gravity of Russian civil society in exile.

Scanning horizons in the field of censorship is not Teplica's first experience with predictive analysis. The first workshop, based on a similar methodology, took place in April 2019, and its results were published in the 2020 issue of Horizon Scanning (available in Russian and English at <https://hs.te-st.org/en/>). That study was about the general spectrum of technologies for civil society and, admittedly, was not wrong in at least part of its observations (in particular, about the role of AI, smart cities, and the role of privacy).

# Trends



Long-term or short-term trends that may influence the future, but may be more local or sectoral (e.g. technological innovation or changes in legislation).

Workshop participants identified trends that could affect the state of censorship in two areas: 1) societal and political trends and 2) technological trends. We read some trends as having a negative impact on Internet freedom (which the researchers particularly emphasized), some as neutral and some as positive. We leave it to readers to determine the trend sign for themselves.

# Trends societal and political

## Possible consequences



### The militarization of public life

Militarization leads not only to an increase in the price of self-expression but also to the strengthening of the "war party," shifting the boundaries of acceptable violence and expanding the number of triggers that trigger this violence. Along with this comes the militarization of the economy and, in the long run, a new wave of property redistribution, repression within the elites, and a partly violent, partly natural (some elites simply leave) change of the elites.



### Reduced transparency of the state apparatus and censorship in particular

Starting in 2022, some "foreign agents" labels were assigned by an "unknown body" (previously, in such cases, it was indicated, for example, "Prosecutor General's Office"). As censorship increases and is more difficult to explain, the transparency of censorship (presented in the form of official registries) will decrease. One can imagine a system of both "exclusion" and "inclusion" lists of blocked websites, the exact content of which will be classified. This, in turn, especially in the media and civil society will lead to a demand for services that automatically detect blockages within the country.



### Increased censorship in education (especially in the humanitarian sciences)

The diversity of viewpoints on a range of subjects and topics is reduced. As a consequence, the practice of critical thinking and free discussion diminishes in students and pupils. The ability to analyze social events in a qualified manner decreases.



# Trends societal and political



The growth of ethnic consciousness in the regions and people's disillusionment with the idea of "putinism"

## Possible consequences

New national movements are emerging in the national republics in Russia, the imperialist perspective on the war in Ukraine is becoming more wide-spread, and the number of criminal cases on charges of calling for separatism is growing. In this connection, we can predict a particular strengthening of censorship in those regions where separatist tendencies might grow faster.



Normalization plays a greater role in limiting information exchange than censorship itself

The emergence of a new "normality" for those living in Russia – brutality and repression will begin to be perceived as normal conditions of life. Normalization, together with the observed increase in escapism ("I've stopped watching the news") and ignoring problematic agendas, will facilitate censorship, as the population itself avoids the "wrong" topics.



The "nationalization" of civil society, the substitution of the narrative

The Teplitsa study shows that the state is actively trying to make a substitution in the field of civil society – to show those communities that support the war against Ukraine as a "true" civil society, while marginalizing civil society that opposed the full-scale invasion. In the same vein, we should expect information campaigns, inspired scandals, and other PR interventions that would emphasize the gap between those who left and those who stayed.



Breaking the usual models of funding media work

Censorship on the one hand and sanctions on the other have seriously affected the way the media make money. Some of the media cannot receive funds from Western sources, while others have lost advertisers inside the country. Researchers suggest that this trend will have a string of consequences. For example, the degradation of the profession: fewer journalists enter the profession than leave it.



# Trends technological

- Increased pressure (both offline and online) on activists and citizens with any active position
- Distribution of video surveillance throughout the country
- Introduction of national certificates and phasing out of international SSL standards
- Movement towards nationalization of personal data storage
- Launch of Russian app marketplaces and displacement of global marketplaces

## Possible consequences

Activists will have to spend more resources on anonymization and combating attacks, which can significantly slow down and even freeze the progress of civil society.

It will become easier for the state to identify any citizens, monitor their movements, and restrict their rights. The path from denunciation to detention will be significantly shortened, which will increase the speed and, potentially, the massiveness of repression.

A sharp decrease in the security of information transfer, the simplification of data interception by the state, the inability to use Russian services without installing national certificates.

The introduction of the obligation to store user data in state-controlled databases will greatly simplify surveillance and profiling<sup>4</sup>. At the same time, we can predict an increase in the number and scale of leaks, which will make Russian citizens defenseless not only in the face of an authoritarian state, but also in the face of criminal structures.

If global marketplaces are replaced by national marketplaces, the state will be able to censor the installation level of applications and introduce surveillance tools into applications.

<sup>4</sup> Profiling is the analysis and interpretation of data to identify characteristics or patterns of behavior, while surveillance is the process of observing and collecting information. However, these concepts may overlap if, for example, the information collected during surveillance is used to create a profile of a person or group of people.

# Trends technological



Implementing machine learning in both censorship and blockchain circumvention

## Possible consequences

The use of artificial intelligence can make it easier for censors to recognize patterns, analyze and "poison" content, create fakes, and analyze behavior, actions, and relationships within activist ranks. On the other hand, these same technologies can serve activists and journalists for deeper research and obfuscation<sup>2</sup> of communications.



Development and implementation of Web 3.0

It will become easier for civil society actors to use the decentralized Internet in terms of storage and communication, and it will become harder to keep track of the decentralized Internet – but it will also increase attempts to regulate it.



Distribution of affordable satellite Internet

The monopoly of control over cross-border data exchange will be called into question by satellite technology. This, in turn, could lead to increased conflicts related to satellites, as well as increased control over user devices equipped with individual cross-border data sharing technologies.



Accessibility of quantum computing

Quantum transition, i.e. the ability to use quantum computing to decrypt existing encryption systems, could call into question the reliability of sensitive information storage and the reliability of those online correspondence protocols (in particular, endpoint encryption) that are now considered secure. This, in turn, could lead to significant threats to domestic activists.

<sup>2</sup> Communication obfuscation (or linguistic obfuscation) is the use of complex, confusing or obscure phrases and terms in order to make it more difficult to understand or to hide the true meaning of the message expressed. It is usually done to confuse or hide information from certain people or groups.

# Trends technological



Preparation for the Splinternet, presented under the sauce of the "sovereignization" of the information space



Reinforcement of primary and secondary sanctions

## Possible consequences

In pursuit of control, censorship and surveillance, the state has the means and motive to develop the Russian Internet toward greater isolation. This movement is likely to be framed in slogans of "sovereignization". Comparing similar trends in other authoritarian countries, Iran and especially China, as well as states loyal to them, may offer the world a splinternet, i.e. the creation of isolated local networks that will lose global connectivity.

Experts observe a rise in prices for new equipment and technology, a decrease in their lifespan, the aging of existing equipment and the increasing complexity of delivery methods. If this trend continues, we can expect a decrease in the quality of Russian services along with an increase in costs - this is already happening in the area of mobile communications. State monopolization of technology imports is possible. It also cannot be ruled out that the only supplier of IT equipment will be China, which will supply equipment with built-in functions of surveillance and remote administration (by the supplier).

# Weak signals



Many "weak signals" will lead nowhere, but others have the potential to be harbingers of events and trends that will influence the development of censorship over time. "Weak signals" have been chosen through the lens of information exchange—which can positively or negatively affect the speed and completeness of that exchange.

Many of the points below are speculative "what if" in nature and seem deliberately unrealistic. In our opinion, it is better to have these unlikely areas of development in front of you. The authors of the report have no advice on what can be done not to turn negative weak signals into catastrophic scenarios.



# Weak signals

## What if?

- **The state will force private companies to monitor employees and locally enforce reprisals**
- **Introduction of profiling and economic sanctions against a disgruntled or "behaviorally deviant" population**
- **The Talibanization of society – the rise of an ultraconservative, fundamentalist agenda**
- **Deprivation of citizenship, property and other rights, denial of consular services to dissidents who found themselves abroad**

## Possible consequences

Private companies will become conductors of repression, will promote the state narrative, the place of work will become a place of surveillance. Another offshoot of this weak signal could be to outsource some of the repression (about the same way the Wagner PMC outsourced the military functions).

The state will be able to automatically impose economic sanctions on the population for behavior on the Internet (analysis of subscriptions, likes, communication) and offline (participation in meetings, rallies and any unauthorized events).

One avenue for limiting information sharing could be a retreat into an ultraconservative agenda, such as that created by the Taliban in Afghanistan. In this case, the state renounces high-tech forms of surveillance and influence and declares war on any technology or manifestation of progress.

At the turn of 2022 and 2023, the media reported that Russian consulates refused to provide services to departing activists with Russian citizenship. In addition, a number of influential State Duma deputies have spoken out in favor of striking people with "foreign agent" status, for example. Risks of kidnapping, arrest, and possibly murder of activists on the territory of other countries will grow. Russian authorities have done this before and can do it again if they wish. If these alarms become a trend, we can expect a reaction in the form of reduced visibility of civil society, especially anti-war movements, for fear of reprisals—even abroad.

# Weak signals

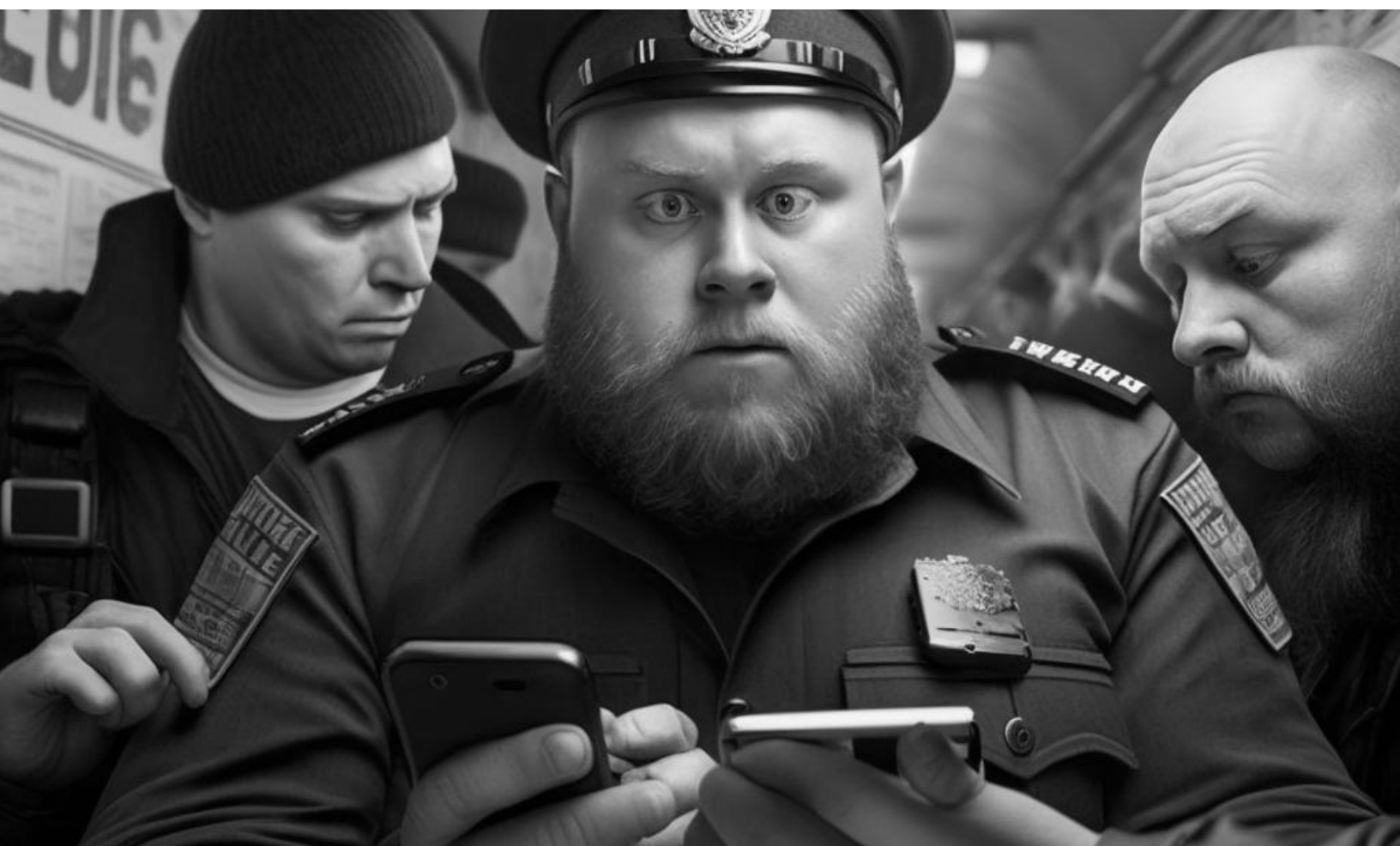
What if?



Changing language along the lines of the linguistic reform after the 1917 revolution

Possible consequences

The Russian language protection law became effective in February 2023, possibly paving the way for further state-led linguistic identity reforms. This could complicate communication with Russian citizens, making it harder to influence discussions within the country



# Pivot points



In the horizon scanning technique, key changes in trends are denoted by various terms: pivot points, bifurcation points, discontinuities. We see these points through the prism that these are relatively short historical moments in which there is an opportunity to choose one path or another. In other words, these are forked points where specific irreversible events or decisions determine the direction of trends.

# Pivot points



Putin's death

## Possible consequences

The struggle for power is not so much at the federal level as in the regions, the growth of separatism up to armed clashes.



Criminalization of content consumption

A sharp decrease in the audience of independent media on all distribution channels.



Ban all user devices that are not certified or registered by the RCN

User devices (computers, phones) without a certificate or registration will not be able to access the Internet. To obtain a certificate, you will need to install software with pre-installed features to monitor traffic and user behavior.



The end of the war in Ukraine

1. The fall of Putin's regime, liberalization, elections, resumption of democratic transit.

2. Reinforcement of the regime. In this scenario, the country will become even more incapacitated, closing itself off from the outside world. The regime will begin searching for internal enemies and a "fifth column," which will intensify repression.



# Conclusion



The future of censorship in Russia depends on a unique confluence of technological and political factors. The implementation of the "Splinternet" scenario could cause profound changes in the global information space, undermining global unity and the possibility of the free exchange of ideas. The adaptability and progressiveness of modern technologies, such as satellite Internet, can be a hope in the fight against censorship.

To successfully resist censorship and preserve information freedom in Russia, one must incorporate creativity by coming up with new and original methods to combat blocking and surveillance. Activists, human rights activists, and technology experts should develop strategies and tools that can circumvent restrictions and preserve the free flow of information. Free flow of quality information that reflects the horrors of the full scale aggression in Ukraine and corruption and moral failure of the current Russian government elites is a necessary element to end the aggression in Ukraine and, possible, start the democratic transition in Russia.

# Acknowledgements



The authors of the report are **Denis Yagodin**, Director of Innovation at Teplitsa, and **Alexey Sidorenko**, co-founder and head of Teplitsa (te-st.org)

The authors would like to thank all the experts who participated in the preparation. In particular:

**Dmitry Vitaliev**, founder and director of eQualitie

**Sarkis Darbinyan**, founder of Roskomsvoboda

**Mikhail Klimarev**, executive director of Internet Protection Society

**Natalia Krapiva**, legal advisor at Access Now

**Anastasia Sergeyeva**, International Secretary of the Citizens Council

**Editor – Nikolay Kononov**, Teplitsa

Report initiator and editor – **Alexey Sidorenko**, Teplitsa

Illustration by **MidJourney**

The text of the report is provided under the **Creative Commons CC-BY 4.0** license