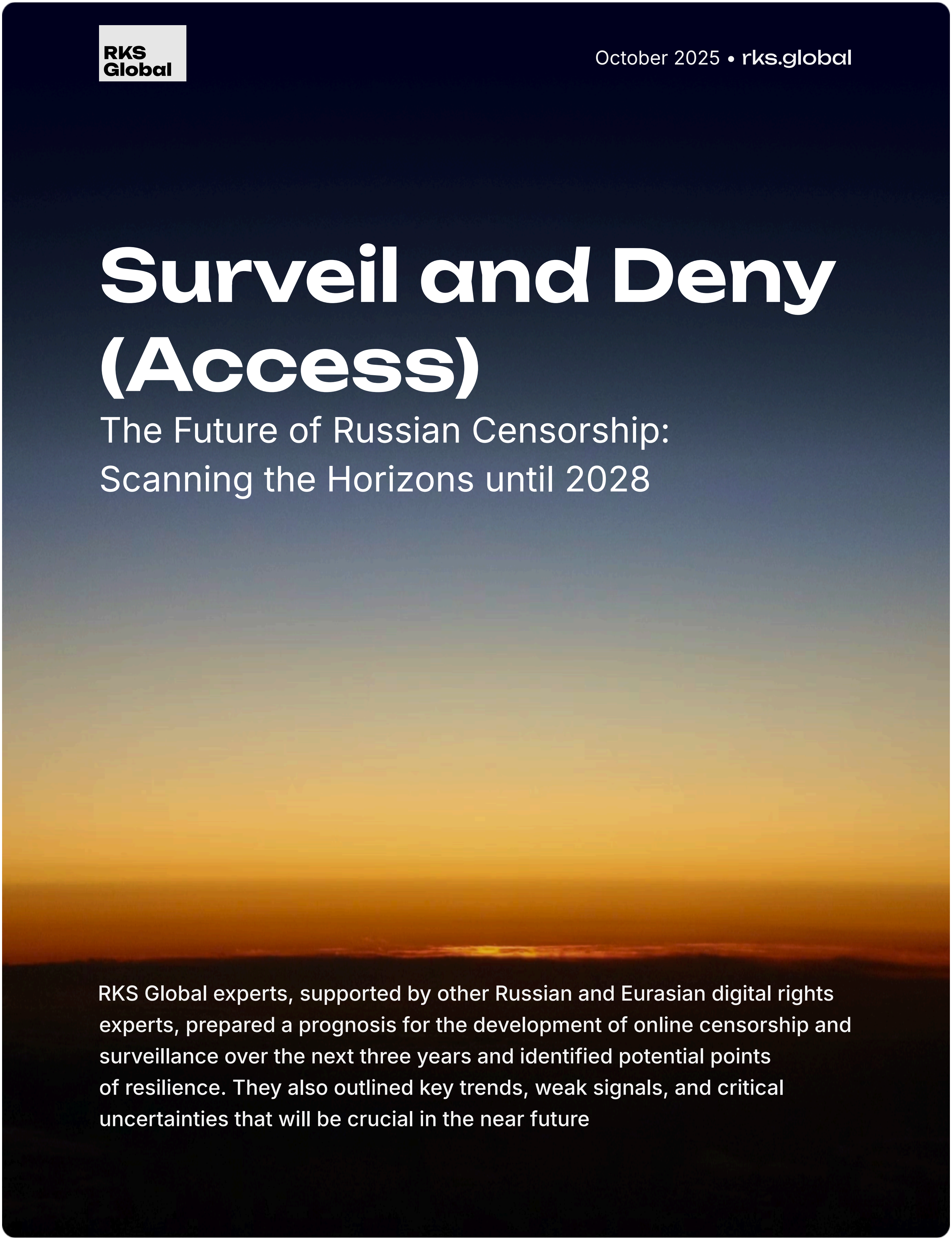

RKS Global

October 2025 • rks.global

Surveil and Deny (Access)

The Future of Russian Censorship: Scanning the Horizons until 2028

RKS Global experts, supported by other Russian and Eurasian digital rights experts, prepared a prognosis for the development of online censorship and surveillance over the next three years and identified potential points of resilience. They also outlined key trends, weak signals, and critical uncertainties that will be crucial in the near future

Executive Summary

1. By 2028, Russia's information control system may ultimately become institutionalized as a tightly regulated, autarkic framework, resembling Turkmenistan's model. Alternatively, it may begin to collapse under its own weight, depending on the sustainability of the regime, citizens' reaction to the implemented measures, the international agenda, and technical capacity of implementers.

2. The global shift toward isolationism and a "rightward turn" create favorable conditions for the strengthening of censorship around the world. International law is experiencing a crisis, the erosion of universal norms and the priority of national digital sovereignty are turning control over information from an exception into a new standard of political stability.

3. Just three years ago, "whitelists" were considered a dystopian scenario. Now, they are becoming part of the new reality, starting as a local experiment and then evolving into a sustainable filtering format. In the future, they may transform from a testing regime into the primary tool of censorship, radically shrinking the space for an independent Internet.

4. Experts emphasize the growing use of artificial intelligence in public control mechanisms, from automated content moderation to network traffic analysis, biometric data and prediction of “unreliable” behavior. Combined with government databases and video surveillance systems, such technologies may form a new level of preventive censorship where intervention starts even before any expression occurs.

5. The future of censorship increasingly depends on unpredictable external factors, such as the war in Ukraine, technological breakthroughs, and generational shifts in society. These factors may not only destroy censorship systems but also change control logic.

Methodology

Forecasts for changes in censorship in Russia for the period 2025-2028 are based on information provided by experts in the field of digital rights and media, lawyers, journalists, and information security specialists.

This document builds on the work of the Teplitsa experts presented in the three-year-old report, "Disconnect and Rule," which was developed using the Horizon Scanning methodology. The 2022 results proved to be highly accurate in predicting subsequent events in the field of Russian state censorship development.

In the new research, experts explored three areas: technological trends, trends in Russia, and global trends. They searched for weak signals, tipping points, and axes of uncertainty — all of which have the potential to radically affect the future of censorship. The experts identified observable trends and prioritized them according to their importance and probability. This approach enabled them to connect observations from various areas—technology, politics, law, and economics—to the overall picture of possible Russian censorship scenarios until 2028.

Trends

Trends are relatively stable, observable over time directions of change in society, technology, economy, politics, or culture. They are characterized by the accumulation of facts and repeatability.

They can be quantitative, such as the growth of AI usage or urbanization, or qualitative, such as a shift in values toward environmental sustainability. Trends do not directly predict the future but indicate the likely trajectories of its development.

Global trends observed outside of Russia

Trend	Possible consequences for global censorship
Aging population in developed countries	Growing conservatism in politics, declining tolerance for risk, and increasing public support for “stability” and “order”; government priorities are shifting from innovation to control.
The "rightward turn” and sovereignty	Strengthening state control over information, establishing national content registries, and restricting external influence on the domestic media market.
Growth of inequality (after the pandemic)	A rise in social tension and protests and, as a result, restrictions on freedom of expression on the pretext of “social stability”.
Focus on safety at the expense of human rights	The prioritization of national security over human rights; the growth of surveillance and justification of censorship through narratives of protection against threats.

Crisis of international law	The polarization of fundamentally different approaches to human rights and, consequently, to the regulation of technologies that directly impact these rights. On the one hand, experts have noted a weakening of international human rights protection mechanisms in several countries and a decline in the effectiveness of international complaints and monitoring of freedom of expression in countries such as China, Russia, and, starting in 2025, the United States. On the other hand, the regulation of content, technology, and artificial intelligence is strengthening and becoming more complicated (the EU).
Transnational repressions/ export of repressions	The expansion of authoritarian states' influence (not limited to Russia) over diasporas, increasing pressure on activists abroad.

Russian socio-political trends

Trend	**Possible consequences**
The expansion of the definition of "Information dissemination organizer" (ORI) to cover all Russian online services	The strengthening of oversight and the obligations to transfer metadata to FSB and Roskomnadzor; the disappearance of private services without state control.
The tightening of border control and digital screening	The transformation of border crossing into a risk procedure; a growing number of personal data leaks resulting from the copying of mobile phone contents; self-censorship and fear of travel.

Increasing self-censorship and ideological conformity	The displacement of independent discourse and adoption of official rhetoric as the new norm; the formation of an atmosphere of voluntary silence and/or ignorance.
The normalization of state practices of Internet shutdowns and “whitelists”	Public acceptance of Internet shutdowns and the degradation of access to Internet services as legitimate measures for the “protection of sovereignty”.

Technological Trends

Trend	**Possible consequences**
Splinternet (Internet fragmentation)	The strengthening of digital borders, restrictions on cross-border information exchange, the development of alternative ecosystems (e.g., the Chinese or Russian Internet). In the West, a reduction in international alliances in the field of digital rights, fragmentation of regulatory approaches, and, as a result, reduced pressure on authoritarian regimes.
Growing global disinformation	A decline in trust in information sources, an increase in manipulative campaigns, and stricter regulations against "fake news" can result in a sharp decrease of trust in any information and, at the same time, to tightening control over media by state actors.
The growing influence of artificial intelligence	Massive automation of content moderation, development of generative media development, public opinion manipulation (such as the poisoning of recommendation models)

	and increased censorship through algorithms; the seamless replacement of banned scenes/content using AI.
Increased transparency of the content moderation system	Pressure on platforms to disclose the functioning of their algorithms, notably, from the EU; the possible emergence of an independent public audit of content moderation.
Growth in global energy consumption	Increased regulation of digital infrastructure and data centers; the emergence of “green” restrictions for large IT projects, including AI models; the migration of services to jurisdictions with sustainable “green” energy; the growing convergence between Big Tech and energy companies, particularly in the field of nuclear energy.
Satellite Internet directly connecting to devices (Direct-to-Device)	On the one hand, a decrease in the effectiveness of national blocking measures and increased access to the independent Internet. On the other hand, the potential development of "national satellite networks" with built-in filtering capabilities.
Commercialization of Space	The privatization of space infrastructure, including satellite Internet, dependence on corporate decisions for civilian access, and increased regulation in the field of orbital communications.
Software import substitution and the implementation of national root certificates	The rise of Adversary-in-the-Middle threats, the risk of emergence of built-in control mechanisms at the device level.
The continued "encapsulation" of Runet and the development	The technical and economic separation of the Runet; deep integration of the FSB with devices (banks, Gosuslugi, Yandex, MAX, Wildberries, etc.); restrictions on access to global services.

of its components (RuStore)	
The expansion of surveillance instruments (SORM, DPI, the Yarovaya law, Option82, facial recognition)	Total transparency of Internet traffic, the creation of centralized profiling databases of citizens, a growing number of data leaks and data misuse.
Whitelists and selective blocking of VPN protocols	The transition from selective to mass blocking, greater difficulty of circumventing censorship, higher costs of digital security for users, and the detection and systematic blocking of VPN protocols and subnets.
The use of cyber forensics technologies (UFED, etc.)	A complete lack of privacy at the border and during detentions.
National DNS and the possibility of cyberattacks such as spearphishing	The centralization of routing, reduced reliability and security of communications; an increase in targeted attacks against Apple/iCloud users and similar services.
The growing number of state-sponsored cyberattacks with a low level of preparation	Increased digital pressure, including the use of hacker attacks as part of transnational repression and possibly even the legalization of these attacks as a special type of operational-investigative activity.
Automation and algorithmization of censorship	Mass implementation of AI content moderation when uploading new content to the network, a decrease in transparency of blockings, the possibility of the instant removal of “undesirable” materials without human involvement. AI errors are becoming a new tool for exerting pressure.
Expanding surveillance tools and identification	The total collection of biometric and behavioral data, the integration of facial recognition into transportation and fintech, the growth of “predictive control,” and, possibly, the

	criminalization of any private communication that law enforcement agencies cannot access.
Export of technologies – “censorship as a service”	The spread of Russian and Chinese information control solutions to third countries; the creation of a market for repressive IT services, where censorship becomes a commercial service.
The transition from self-regulation to state regulation of moderation	The disappearance of independent moderation and codes of conduct on major Russian tech platforms, the direct accountability of these platforms to the government, and the increased censorship under the pretext of “establishing order.”
The introduction of a new form of controlled money (CBDC)	The introduction of programmable money that can only be spent on purposes specified in a smart contract; the erosion of banking secrecy; the destruction of financial anonymity, and, consequently, restrictions on donations and the purchase of technologies prohibited by the state; a parallel ban on the free circulation of cryptocurrencies.

Weak signals

Weak signals are early, often scattered, and imperceptible indicators of potential meaningful changes. These phenomena have not yet taken root in the mainstream and may seem random. They are most often found on the periphery, in areas such as research, prototypes, niche practices, and cultural experiments. Their value lies in their ability to anticipate new trends or turning points. The table below lists socio-political and technical trends.

Weak signal	Why it is important/ Possible consequences
Pro-government elites on the foreign agents list	The erosion of the initial meaning of the foreign agent concept and its transformation into a tool for internal conflict among elites. A possible transition to "overall susceptibility" and a reduction in political loyalty within the system.
Kazakhstan and Belarus are moving away from Russia's sphere of influence	The weakening of Russian regional hegemony in the post-Soviet space. The strengthening of Belarus' European integration, more independent policy in Kazakhstan. These changes will lead to tighter control over Russia's domestic agenda and stricter censorship to maintain legitimacy. Coups, blackmail (as in the case of Azerbaijan), and a Georgian scenario (supporting a Kremlin-loyal party in elections) cannot be ruled out.
Self-hosted LLMs against censorship	The emergence of user-based AI systems that do not depend on centralized platforms threatens the monopolization of information control. Possible new bans and regulations of open-source models.
The strengthening of BRICS	The establishment of an alternative center of power with its own digital standards and censorship

	protocols. The emergence of an “anti-Western” model of Internet governance.
Deprivation of citizenship	A new form of political repression and a tool for expelling those who dissent. It creates an environment of fear and encourages self-censorship, even beyond the country's borders.
Depression is a new norm in Russia	Psychological apathy within society makes censorship less noticeable and more effective, as people stop actively seeking alternative information.
Anti-immigration attitudes	The rise of xenophobia and suspicion within society, the emergence of new “internal enemies.” Can be used by the authorities to divert attention from socio-economic problems.
New cultural policy — Social Realism 2.0 / anti-universalism	A return to ideological art, control over cultural production and education. The shaping of a “patriotic” aesthetic canon.
The immortality of dictators	Propaganda myth-making, the use of digital technologies (deepfakes, AI avatars) to extend leaders' symbolic presence. The cult of personality is strengthened.
The redistribution of property	The confiscation and redistribution of assets in favor of loyal elites. Businesses are becoming more dependent on the state; economic censorship is growing (through pressure on media and IT company owners). A redistribution of the Russian big tech and telecoms market cannot be ruled out.

Tipping points / inflection points

Tipping points / inflection points are moments or states of a system after which further development dramatically changes. This is often a point for irreversibility: a small impact triggers large-scale consequences. For example, the mass adoption of smartphones in 2007–2010 was a tipping point for the digital economy. A tipping point can turn a weak signal into a dominant trend.

Tipping point	Possible consequences
Putin's, Trump's or other leaders' death → change of regime(s)	Radical political shifts, the destabilization or liberalization of regimes, changes in international alliances, temporary chaos in foreign policy.
USA-China war (Taiwan)	A crisis in global trade, the collapse of global supply chains, increased militarization and digital control, and the accelerated formation of new blocs (US–EU vs. China–Russia).
Ceasefire / end of the war in Ukraine	The restructuring of Europe's security system, partial normalization of sanctions policy, and the return of international investment to the region. However, there is also the possibility of political revanchism by Russia.
Invasion of Russia to Europe	NATO mobilization, the declaration of a state of emergency in the EU, the collapse of diplomatic relations, the transition to a wartime economy.

Runet whitelists as a single form of censorship	At the time of writing, "whitelists" were a rare measure used only in a few regions. However, the development of this form of censorship into the primary method of controlling information exchange will be a serious turning point. It will require rethinking work models for independent media outlets, civil society organizations, and neighboring countries' policies toward Russia. Along with news for the Russian population, news about the country will significantly decrease.
Emergence of Artificial Super Intelligence (ASI[1])	The loss of human control over AI, the redistribution of power from states to corporations or systems, and radical shifts in economics and work relationships, such as mass unemployment and global impoverishment of the population.
A new pandemic/ Black swan event	New forms of biocontrol, increased biometric surveillance, the rise of authoritarian practices under the pretext of security, changes in global health priorities.
Economic/banking crisis	Mass unemployment, currency and market crashes, the rise of radical political movements, declining trust in institutions, and the growth of cryptocurrencies and alternative economies.
Repeal of the moratorium on the death penalty (global totalitarian shift)	The establishment of police states, shrinking of civil rights, and the initialization of fear as a management instrument.
Quantum computer	The breakdown of existing cybersecurity systems, a new wave of technological competition, and the redistribution of power among technological superpowers.

[1] Artificial Super Intelligence (ASI) is a hypothetical form of artificial intelligence that surpasses the human mind in all areas and is capable of self-improvement.

Nuclear war/strike	A global catastrophe, a radical reduction in population, the destruction of infrastructure, a new world order built on the ruins of the existing one.
Emergence of cyborgs	The blurring of boundaries between humans and machines, ethical and social crises, unequal access to “improvements,” and the emergence of new forms of discrimination.

Axes of Uncertainty

Axes of Uncertainty are key factors of the future that cannot be used to make a confident forecast but which can radically affect future scenarios. They are critical uncertainties that set the framework for alternative futures, not just "unknowns." Usually, two to three axes are identified to build scenarios, such as: "level of international cooperation — high or low" and "pace of AI implementation — fast or slow." The combination of variances creates a matrix of scenarios.

Axe of Uncertainty	Two poles (possible states)	Importance for censorship and the information environment
The war in Ukraine	Ongoing/ ended	During wartime, there is a maximum militarization of the information field, including censorship, blocking, and criminal cases for "discrediting the army." If the war ends, there is an opportunity for the liberalization of information exchange, perhaps as a condition for lifting sanctions.

International isolation	Deep/ low	The loosening of international sanctions could have contradictory effects. On the one hand, weaker sanctions could lead to the expansion of the censorship system through the purchase of Western equipment. On the other hand, if sanctions are lifted against a backdrop of liberalization, the "thaw" in the West may correlate with a "thaw" in Russia.
Regime sustainability	Stable/Unstable	The parameter of regime sustainability remains one of the axes of uncertainty (especially in the context of the outcome of the war with Ukraine). If the regime remains stable, it is unlikely that the situation with censorship will improve. If instability increases, it is clear that even with the willingness to control the uncontrollable, resources to restrain the free flow of information will simply be insufficient.
Technological capacity	High/low	Experts do not have a clear understanding of Roskomnadzor's and other services' real technical capabilities, especially in the context of sanctions, to implement truly dystopian technologies. If the statements made by Roskomnadzor, the FSB, and others are true, then the most alarming predictions may materialize. However, if these statements turn out to be mere vanity, the feasibility of the most draconian measures will most likely be significantly reduced due to incompetence and a lack of human resources.