


Russia's securitised approach to AI sovereignty


Alexander Ignatov

Senior Research Fellow, Center for International Institutions Research, Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow; and Visiting Scholar, CyberBRICS project, Center for Technology and Society (CTS), Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro

 <https://orcid.org/0000-0001-6740-4454>

Danil Kerimi

Doctoral Candidate, School of Social Sciences and Technology, Technical University of Munich

 <https://orcid.org/0009-0002-7235-4257>

Abstract

In the context of the world's major powers competing for dominance in the artificial intelligence (AI) realm, Russia aims to become a global leader in AI development. This article evaluates Russian AI governance through the lenses of the key AI sovereignty enablers (KASE) framework and the Copenhagen School's securitisation theory. The Russian government's approach to AI governance, in line with its broader approach to digital governance, grants extensive powers to state security and law enforcement entities, while major domestic AI market players are state-influenced. This securitised approach to AI sovereignty and governance stems from concerns about the country's stability, alongside a high degree of politicisation of digital governance. The article argues that the likely impact of Russian securitisation of AI governance will be further consolidation of state control over AI innovations and a narrowing of the space for non-state technological developments.

Keywords

Russia, artificial intelligence (AI), AI sovereignty, securitisation, digital economy

DOI: <https://doi.org/10.23962/ajic.i35.20626>

Recommended citation

Ignatov, A., & Kerimi, D. (2025). Russia's securitised approach to AI sovereignty. *The African Journal of Information and Communication (AJIC)*, 35, 1–11. <https://doi.org/10.23962/ajic.i35.20626>



This article is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence:

<https://creativecommons.org/licenses/by/4.0>

1. Introduction

As the heir to the Soviet Union's scientific legacy, Russia has been keen to highlight its modern digital power and its prominent global AI ambitions. As an integral component of the country's efforts towards digital sovereignty, AI-based solutions attract growing attention from Russia's leadership, as exemplified by an ambitious agenda in terms of which Russia is to reach the top ranks of global AI powers by 2030 (President of Russia, 2019b). Nonetheless, in addition to the already tough competition for global AI leadership, Russia's efforts are further complicated by geopolitical/military conflict and economic sanctions.

In this study, we reviewed Russia's efforts to achieve AI sovereignty through the lens of Belli's key AI sovereignty enablers (KASE) framework (Belli, 2023), which is grounded in Belli's (2023) framing of AI sovereignty as "the capacity of a given country to understand, develop and regulate AI systems" (2023, p. 1). We also reviewed Russia's AI governance through the lens of securitisation theory, as set out by the Copenhagen School (Buzan et al., 1998). This securitisation lens allowed us to explore the differentiated weight that the Russian government places on the KASE dimensions.

As set out in this article, we found that, as a product of Russia's current geopolitical context, AI is often viewed by the country's leadership as a national military, political, and economic security priority, i.e., AI is viewed as a security/securitisation matter. Consequently, the state actors that deal with cyber, information, data, and energy security matters are given considerable financial support. We conclude that it is highly likely that, in the foreseeable future, the under-prioritised (from the securitisation perspective) dimensions will follow the same path, thus completing the securitisation of AI within Russia's public discourse and policy framework. This article also provides insight into the general stance of Russia's leadership towards emerging AI-based solutions and potential approaches to the development of a market regulatory framework.

2. Challenges to Russian AI development

Russia's proclaimed goal to become a global AI leader aligns with the country's overarching ambitions of building a strong digital state (President of Russia, 2019b). Russia's political and economic elites are determined not to miss out on current technological trends that are firmly driven by AI. In the 2020s, the laissez-faire approach to digital regulation ended in many parts of the world. Russia is among the countries taking control of the next stage of technological evolution—away from the business community and towards the state (Zinovieva, 2024). However, Russia is faced with additional challenges in respect of talent, compute power, and capital dimensions. These challenges include: the brain drain due to fears generated by the conflict with Ukraine, an underdeveloped hardware ecosystem, and budgetary pressures due to sanctions and competing investment priorities.

According to a statement on the recently approved state budget proposal for 2025, Russia is increasing its military budget by 25% to RUB13.5 trillion (USD145 billion), which is equivalent to 6.31% of the country's GDP (Miller, 2024). As the military budget grows, other areas will inevitably suffer. Thus, according to the same budget proposal, civilian research will shrink by a quarter (Statista, 2024). According to the Institute for Statistical Studies and Economics of Knowledge of the Russian Higher School of Economics, the RUB458 billion (USD4.9 billion) that was dedicated to applied research in 2024 will be reduced to RUB362 billion (USD3.5 billion) in 2025, and to RUB260 billion (USD2.6 billion) in 2026 (Gerden, 2024). To put these figures into perspective, Google's parent company Alphabet alone spends 10 times more than Russia on applied research. In dollar terms, Russia will spend about the same amount on combined research and development (R&D) in 2025 as Portugal. On average, in recent years, Russia has spent about 1% of its GDP on R&D activities. This is less than what is spent by countries such as Malaysia and Egypt and is less than half of the average in Organisation for Economic Co-operation and Development (OECD) countries (OECD, 2023).

For Russia's Federal AI Programme, the same budget proposal provides RUB1.145 trillion (USD11.5 billion) allocated in 2025, which is similar to what is spent annually on R&D by a single Chinese technology conglomerate, Tencent (2024). For 2026, the budget projects RUB1.25 trillion (USD12 billion) and in 2027 RUB1.5 trillion (USD14 billion) (D-Russia, 2024). At the same time, however, additional funds will be allocated to defence-related AI through the aforementioned increased military budget.

In addition to financing AI development, another challenge faced by Russia is an AI talent shortage. In 2022–23, the outflow of IT specialists was estimated at more than 20,000 individuals (*Realnoye Vremya*, 2024).¹ Another estimate claimed that, in the first half of 2022, the outflow number surpassed 40,000 (RBC, 2022). The Ministry of Digital Development, Communications and Mass Media reported that, in 2022, at least 100,000 IT specialists left the country and only 10,000 returned (Inclient, 2022). While some of the leading Russian software companies claim that the outflow of IT specialists is not affecting them (Telecom Daily, 2024), the labour market shows a growing demand for specialists with no considerable or even any relevant experience, as hiring requirements soften to accommodate the shortage of personnel. In Tatarstan, where one of the biggest Russian IT hubs, Innopolis, is located, the growth in demand for IT specialists has been estimated at 103% (*Realnoye Vremya*, 2024).

¹ The shortage of capable AI specialists was on the agenda even before this period (see Nadibaidze, 2022).

Perhaps the biggest challenge that Russia must overcome on the road to a robust AI development ecosystem is the lack of hardware availability. This inherited weakness of the Russian computing ecosystem has been further worsened by the sanctions imposed by foreign countries (Kolomychenko, 2024). Russia's domestic production of electronic components is negligible by global standards. Within the framework of the state programme to support the electronic industry, projects such as the Baikal microprocessors production facility (Baikal Electronics, n.d.; Bendett, 2024) have been implemented to organise the production of microprocessors using domestic technologies, with progress towards localisation of the production chain announced in March 2024 (Kholupova, 2024). Nevertheless, the main production of Russian processors continues to be outsourced to labs outside the country, such as Taiwan's TSMC (Urusov, 2023).

Russia's major digital market players are either state-owned or have significant ties to the state, which means that commercial practices are often influenced by the state's national digital-sovereignty priorities (Petrella et al., 2021). For instance, Russian IT companies are, as in most other countries, obliged to give law enforcement and intelligence agencies access to users' data only with court authorisation. However, there are frequent reports in the independent media of Russian digital platform firms such as VK granting access to users' data based on a simple "telephone call" from a law enforcement or intelligence agency—even when such data transfer should result in a criminal prosecution for the firm concerned (Sidelnikova, 2024).

3. Analytical tools: The KASE framework and securitisation theory

We deployed two analytical tools in our evaluation of the state of Russian AI governance: the KASE framework and securitisation theory.

KASE framework

The KASE framework put forward by Belli (2023) sets out eight dimensions as crucial to a country's progress towards AI sovereignty:

- data governance;
- algorithmic governance;
- computational capacity;
- meaningful connectivity;
- reliable electrical power;
- digitally literate population;
- strong cybersecurity; and
- appropriate regulatory framework.

In our KASE evaluation we used a mapping tool (see Appendix) that we developed with colleagues in the CyberBRICS project (CyberBRICS, n.d.).

Securitisation theory

In addition to the KASE framework and mapping, we see securitisation theory as a useful analytical lens for exploring AI sovereignty dimensions in various countries, and particularly in Russia (Stix, 2022). In many countries, the officials who are now dealing with AI regulation were previously in charge of cyber policy (Ünver, 2024). Cyber policy, for its part, was in many cases built upon counter-terrorism work (UNICRI & UNOCT, 2021a; 2021b). Since the early 2000s, at national and international levels, the work of counter-terrorism experts has been compelled to evolve into AI-focused responsibilities. A line can be traced from post9/11 (2001) counter-terrorism capacity-building through to cybersecurity regimes (e.g., the Tallinn Manual and DHS cyber strategies), with personnel and frameworks then migrating, both operationally and institutionally across national and multilateral levels, into the nascent domain of AI governance (Bianchi & Greipl, 2022; Pfaff, 2025; Tallberg et al., 2023; US Department of the Treasury, 2024).

For example, the G7's 2023 AI Principles emphasise AI security risk management and trace their heritage to cybersecurity norms originally designed for counter-terrorism-inspired threats (EC, 2023). Similarly, OECD statements underscore growing synergies between cybersecurity and AI governance, shaped by counter-terrorism risk frameworks and cyber-risk protocols (OECD, 2024). Meanwhile, in the private sector, those

overseeing, for instance, anti-money laundering in the financial services sector, are the ones at the forefront of AI adoption with significant technology budgets (US Department of the Treasury, 2024).

Securitisation theory is closely associated with works by Buzan, Wæver, and de Wilde, collectively referenced as the Copenhagen School (Buzan et al., 1998). The theory explains how a part of objective reality becomes viewed as a threat to a referent object, e.g., a state, a person or a group of people dependent on a sphere of interest, namely the economy, society, the military, policy, or the environment. Grounded in identification of the threat by the state, securitisation presents an argument whereby the state advocates implementation of extraordinary measures to counter the threat, even when the measures may contradict established rules. Securitisation can also be viewed as the process by which non-politicised issues (issues not talked about, or not part of public debate) or politicised issues (issues already publicly debated) are elevated to security issues that need to be dealt with as a matter of urgency and that require bypassing of procedures for public debate and democratic engagement.

According to Charrett (2009), a prominent example of a securitised issue is terrorism. The dramatic changes in US foreign policy after the 9/11 attacks of 2001, which eventually resulted in a US-led invasion of Iraq in 2003, became possible due to US President George W. Bush's use of enhanced executive powers grounded in a securitisation of the "meaning of 9/11" (Charrett, 2009) as something requiring harsh, responsive actions by a state unfettered by normal procedural checks and balances. The proclamation of the US response to 9/11 as a "Global War on Terror" (National Archives, n.d.) led to significant expansion of presidential powers, spying on ordinary Americans, detention of Muslims and Arabs, and establishment of a secretive military tribunal system—with most of these elements remaining in place despite protracted debate and sustained efforts to roll them back in order to ensure the separation of powers and stability of the democratic order (Charisle, 2021).

In summary, a completed securitisation means that: (1) the state provides the public with an argument framing a referent object as threatened; (2) there is a stated demand to exercise extraordinary measures to protect the referent object; and (3) justification is provided for the state to break established rules in order to protect the referent object. In this study, we employed the securitisation lens as a means to explore bureaucratic and structural tendencies in the Russian state's approach to AI development, and to build a picture of the future of the country's AI governance model.

4. KASE findings

Data governance

Russia does not have a specialised data governance strategy, but it has a comprehensive framework with clearly assigned responsibilities and practical regulatory systems. The Ministry of Digital Development, Communications and Mass Media leads data management, security, and regulatory policies, alongside Roskomnadzor (the Federal Service for Supervision of Communications, Information Technology and Mass Media) and the Federal Security Service (FSB). The primary data governance law is the Federal Law on Personal Data (No. 152-FZ) (Russian Federation, 2006), supported by additional laws on information and critical infrastructure protection (an overlap with the cybersecurity domain). Core funding comes from government-affiliated funds such as the Russian Science Foundation and the Skolkovo Foundation.

Although Russia lacks an explicit international strategy for AI and data governance, its stance in the international arena—in institutions such as BRICS, the G20, and the UN/UNESCO—has some fundamental features that can be taken as bearing strategic significance, namely Russia's adherence to state-centric multilateralism and its rejection of multistakeholder approaches in which states and non-state actors cooperate.

Algorithmic governance

Leading Russian national enterprises such as Sber (GigaChat), Yandex (Neuro) and VK (all three are directly or indirectly managed by the government) have developed their own large language models (LLMs) and drive AI innovation in Russia, alongside a growing AI startup ecosystem that often collaborates with larger corporations and research institutions. Although an "algorithm strategy" is not specified, the National

Strategy for the Development of Artificial Intelligence (President of Russia, 2019b) emphasises deploying algorithms in priority spheres such as healthcare, education, and transportation, with involvement from government agencies such as the Ministry of Science and Higher Education and the Ministry of Digital Development, Communications and Mass Media. At the time of writing, in early 2025, AI regulation discussions were ongoing in Russia's State Duma (the Parliament's lower chamber), particularly around matters of transparency and accountability, but comprehensive algorithm-specific or LLM-focused laws had yet to be promulgated.

Computational capacity

Russia's Strategy for the Development of the Electronic Industry until 2030 (Government of Russia, 2020) emphasises expanding hardware production, including storage solutions and server hardware, with multiple ministries involved, led by the Ministry of Industry and Trade. Import substitution is a priority, targeting the production of processors, controllers, and memory, and the advancement of silicon technologies to the 5 nanometre (5nm) level for eventual domestic production. State funding for AI and microelectronics R&D has begun to increase significantly, with 2024 investments reaching RUB5.2 billion (USD51.6 million) for AI projects (Norem, 2024). Russia has six supercomputers in the global TOP500 index, with Yandex's Chervonenkis ranked highest among the six, in 75th position globally (TOP500, n.d.). Government-supported enterprises such as Rostec, and private-sector-led (with varying degrees of state ownership) entities such as Sber (50% state-owned), drive growth in computational capacity in the domestic AI sector.

Meaningful connectivity

Infrastructure is considered a backbone of Russia's security, grounded in the notion of "critically important information infrastructure" (Consultant Plus, 2017). The FSB is directly involved in providing protection for critical information infrastructure. The International Telecommunication Union (ITU) (n.d.-a) ranks Russia highly for internet affordability, with the country offering some of the lowest internet costs globally. In 2024, the entry-level fixed-broadband basket cost in Russia was 0.57% of GNI per capita, compared with the global average of 2.66% (2023) (ITU, n.d.-b). Over 92% of the Russian population (with both genders equally represented) use the internet regularly, with 83.1% of rural households and 89.5% of urban residents having internet access at home. Younger users (aged 15–24) have a high internet usage rate (98.7%), while engagement is lower (89.2%) among older generations (25–74 years). Russia's Strategy for the Development of the Communications Industry until 2035 (Government of Russia, 2023), led by the Ministry of Digital Development, states that the fixed telecommunications sector needs more investment due to high costs and potential infrastructure challenges. Russia is connected to multiple submarine cables, most of them domestic, with several of the domestic cables, such as the Polar Express, designed to enhance internal connectivity across regions.

Reliable electrical power

According to the International Energy Agency (IEA, n.d.), Russia's electricity production primarily depends on natural gas (45.1%), with nuclear energy (19.4%), hydropower (17.3%), and coal (16.3%) also playing significant roles. Renewable energy, comprising wind and solar, contributes a small share (3.54% in 2021). The Strategy for the Development of the Electric Power Industry of the Russian Federation (Government of Russia, 2013) aims to modernise and diversify the energy sector, with oversight by the Ministry of Energy. Key regulatory bodies include the Federal Grid Operator, which manages electricity transmission, and the Federal Antimonopoly Service, which maintains competition in the electricity market. Electricity market regulation and the energy industry stability at large are considered matters of utmost importance, with national security concerns involved (Government of Russia, 2019).

Digitally literate population

In 2023, Russian President Vladimir Putin directed an update to Russia's National Strategy for the Development of Artificial Intelligence through 2030 (President of Russia, 2019b), emphasising support for AI research centres along with increased government expenditure. The Russian AI market grew by 18% in 2022, reaching RUB650 billion (USD6.4 billion) (Consultant Plus, 2017), and the government planned to invest RUB5.2 billion (USD51.6 million) in AI in 2024 (Interfax, 2025). The AI Strategy promotes comprehensive AI education, aiming to integrate AI topics across educational levels, to develop specialised degrees, and to

enhance practical training. By 2023, Russia had approximately 17,000 AI graduates (2021–2023) (ComNews, 2024), 70% growth in AI publications in top-tier journals (2019–2023) (Analytical Center, 2024), and 96 approved AI standards (2019–2023) (Government of Russia, n.d.).

The Ministry of Science and Higher Education is tasked by the National Strategy with implementing educational aspects, supported by partnerships with major universities. Furthermore, Russia's AI Alliance, including major tech firms such as Sber and Yandex, supports talent development initiatives (AI Alliance Russia, n.d.). Due to geopolitical tensions, international AI collaboration is limited, with BRICS serving as the primary partner. Russia is aiming for a significant rise in AI-skilled graduates and high AI-readiness across priority economic sectors by 2030 (President of Russia, 2019b), but the lack of skilled labour, mentioned earlier in this article, constitutes a significant obstacle in this respect.

Strong cybersecurity

In Russia, cybersecurity is guided by the National Security Strategy (President of Russia, 2021) and the Doctrine of Information Security (President of Russia, 2016), with the country's Security Council playing a central role in strategy oversight. Regulatory entities, such as Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass Media) and the Cybersecurity Department in the Ministry of Digital Development, are responsible for enforcing cyber regulations. Government funding supports R&D to reduce reliance on foreign technology, focusing on building a skilled domestic workforce and domestic cybersecurity solutions. Geopolitical pressures have led the country's private and public sectors to favour Russian-developed technologies (ComNews, 2023), with companies like Kaspersky Lab and Positive Technologies leading the industry (Kurasheva, 2023).

Appropriate regulatory framework

At the time of writing, in early 2025, Russia had not yet enacted any significant regulation targeting AI. The State Duma's major party *Edinaya Rossiya* (United Russia) is said to have been working on a draft law on AI regulation since 2023—a law that would, inter alia, define AI solutions developers' responsibilities and prevent the use of AI for fraud (*Kommersant*, 2023). Also, in 2023, a draft law was presented to protect AI users against harm arising from AI. In July 2024, President Putin promulgated a law forcing AI developers to provide insurance against possible harm caused by their AI-based products (TASS, 2024). In early 2025, the State Duma created a working group on AI that has a mandate until 2026 to develop regulations (Dorofeeva et al., 2025).

5. Securitisation findings

AI technologies are often viewed as a source of threat to Russia's sovereignty and, especially, to the country's military security. According to President Putin, AI development "shall be constrained" as it would "inevitably lead to a point where they [AI technologies] may begin to pose a threat to humanity—comparable to the development of nuclear capabilities", with national governments around the world taking the lead in the process (President of Russia, 2023). AI as a threat is presented in the national AI strategy, e.g., the 2019 Presidential Decree (with 2024 amendments) approving the strategy includes a notion of AI as a tool for spreading "prohibited information" (President of Russia, 2019b; 2024).

Under Russia's current AI policy dispensation, most of the KASE framework dimensions are either already viewed through the securitisation prism or are on track to soon be viewed in such a manner. An important factor to consider in this process is the balance of power between ministries/agencies subscribing to securitisation and those subscribing to development, i.e., the guns versus butter paradigm. As in other parts of the Russian regulatory and budgetary apparatus, the *siloviki* (security agency personnel) at entities such as the FSB are partly responsible for data governance and cybersecurity policy implementation.² The aforementioned Roskomnadzor serves as a media supervisor and is also deeply involved in data governance. Meanwhile, the market champions include state ownership stakes and operate under state supervision, e.g., Sber, formerly Sberbank and by far the largest Russian bank (Ross, 2024); VK, the largest

2 There is a widespread belief among scholars and policy experts that the influence of Russian security agencies extends broadly across the country's entire IT sector (see Epifanova & Dietrich, 2022).

Russian social media platform (SimilarWeb, 2021); and Yandex, the largest Russian search engine, with 72% of Russia's market share. This supervision is conducted either directly, when the state enacts its powers as an owner, e.g., in Sber, with 50% of its shares owned by the state (Petrella et al., 2021); or indirectly, via proxy "oligarchs", who are company owners tied to the state. The major funds supporting prominent innovation projects are mostly affiliated with the state.

As reliable energy supply has become a major concern for the development of AI worldwide, Russia is not unique in considering energy market stability as a matter of highest importance for AI development. Like other energy-rich countries (e.g., Saudi Arabia, the US), Russia seeks to showcase its capabilities as an "energy superpower"—referring to its ability to influence the global energy market and, in turn, the international agenda (Rutland, 2008). Russia's Energy Security Doctrine of 2019 (President of Russia, 2019a) cites shrinking external markets, difficulties in reaching new markets, and the international climate and environmental agenda as major threats to the country's stability. Also cited in this Doctrine is the wrongful use of information and communication technologies (ICTs) against information infrastructure in ways that may hamper the functionality of energy facilities.

At the time of writing in early 2025, the only examples of non-fully securitised KASE dimensions that our study had identified were (1) algorithmic governance; and (2) the regulatory framework. With respect to both these dimensions, the discussions that were in progress indicated that security considerations were poised to take the lead. Russian algorithmic governance, which some might view as an area characterised by public-private dialogue aimed at finding an appropriate common ground, is in reality a domain heavily influenced by the state, with IT champions serving as proxies. Once this dimension is fully recognised as a potential threat to stability, it is very likely that algorithmic governance will follow the same path as data governance, i.e., politicisation, followed by securitisation. With respect to the regulatory framework, the scarce insights available in early 2025 regarding the ongoing discussions of the AI draft law suggested that security matters were likely to prevail over market interests.

6. Conclusion

Russia aspires to reach a leading position among global AI powers. However, the country's ambition is constrained by shortages of available resources, including compute power, capital and talent. A distinct feature of Russia's AI governance model is the strong influence of law enforcement bodies, namely the FSB and Roskomnadzor, in AI governance. This influence, which goes beyond these agencies' basic responsibilities, serves as an illustration of the ongoing securitisation of numerous aspects of the country's digital-economy governance. Digital technologies, and AI in particular, are viewed by the Russian leadership as sources of risk. The response is the government's politicisation and securitisation of AI-related matters and its supervision of non-state market actors' activities. We expect that the coming years will see more restrictions imposed by the government, justified by the state as a means to protect Russia's AI sovereignty and broader digital sovereignty. The likely impact of the restrictions will be further marginalisation of non-state actors in the Russian AI sector, thus consolidating state control over digital innovation and narrowing the space for open technological development.

Acknowledgement

The authors acknowledge the support of the CyberBRICS project, Center for Technology and Society (CTS), Fundação Getulio Vargas (FGV) Law School, Rio de Janeiro.

Funding declaration

The research was conducted as part of the CyberBRICS project's fellowship programme.

Data availability

The data supporting the results of this study is available upon written request to the first-listed author at ignatov-aa@ranepa.ru.

AI declaration

The authors did not use any generative AI tools for the research covered in this article or in the preparation of this article.

Competing interests declaration

The authors have no competing interests to declare.

Author contributions

AI: conceptualisation; methodology; validation; writing – the initial draft (including substantive translation).

DK: conceptualisation; data collection; validation; writing – revisions.

References

- AI Alliance Russia. (n.d.). *AI Alliance Russia*. Retrieved April 8, 2025, from <https://a-ai.ru/?lang=en>
- Analytical Center. (2024). *2024 Analytical report on publication activity of Russian specialists at A* level conferences in the field of artificial intelligence for the period from 2019 to 2023*.
- Baikal Electronics. (n.d.). *About the company*. Retrieved November 20, 2024, from <https://www.baikalelectronics.ru/about/>
- Belli, L. (2023). *Exploring the key AI sovereignty enablers (KASE) of Brazil, towards an AI sovereignty stack*. <https://cyberbrics.info/wp-content/uploads/2023/08/AI-sovereignty-updated-CLEAN.pdf>
- Bendett, S. (2024). *The role of AI in Russia's confrontation with the West*. Center for New American Security (CNAS). <https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west>
- Bianchi, A., & Greipl, A. (2022, November 17). *States' prevention of terrorism and the rule of law: Challenging the "magic" of artificial intelligence (AI)*. International Centre for Counter-Terrorism (ICCT). <https://icct.nl/publication/states-prevention-terrorism-and-rule-law-challenging-magic-artificial-intelligence-ai>
- BRICS. (2024). XVI BRICS Summit Kazan Declaration. <http://static.kremlin.ru/media/events/files/en/RosOySvLzGaJtmx2wYFv0IN4NSPZploG.pdf>
- Buzan, B., Wæver, O., & de Wilde, J. (1998). *Security: A new framework for analysis*. Lynne Rienner.
- Charisle, M. (2021, September 11). How 9/11 radically expanded the power of the U.S. government. *TIME*. <https://time.com/6096903/september-11-legal-history/>
- Charrett, C. (2009). *A critical application of securitization theory: Overcoming the normative dilemma of writing security*. Working Paper No. 2009/7. International Catalan Institute for Peace. <http://dx.doi.org/10.2139/ssrn.1884149>
- ComNews. (2023, May 25). *57% of Russian companies have switched to domestic software*. <https://www.comnews.ru/projects/import-substitution/news/226354/57-rossiyskikh-kompaniy-pereshli-otechestvennoe>
- ComNews. (2024, March 22). *With the growing demand for AI specialists, only a few Russian universities are graduating qualified personnel*. <https://www.comnews.ru/content/232211/2024-03-22/2024-w12/1007/pri-rastuschey-potrebnosti-specialistakh-ii-tolko-neskolko-rossiyskikh-vuzov-vypuskayut-profprigodnye-kadry>
- Consultant Plus. (2025). *Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation" dated 26.07.2017 N 187-FZ (latest revision)*. https://www.consultant.ru/document/cons_doc_LAW_220885
- CyberBRICS. (n.d.). *About us*. <https://cyberbrics.info/about-us>
- Dorofeeva, E., & Arialina, M. (2025, April 8). The State Duma has created a working group to regulate artificial intelligence. *Vedomosti*. <https://www.vedomosti.ru/society/articles/2025/04/08/1103157-v-gosdume-poyavilas-po-regulirovaniyu-iskusstvennogo-intellekta>
- D-Russia. (2024, October 1). *What digital expenditures are included in Russia's draft budget for 2025-27?* <https://d-russia.ru/kakie-cifrovye-rashody-zalozheny-v-proekte-bjudzheta-rossii-na-2025-27-gg.html>
- Epifanova, A., & Dietrich, P. (2022). *Russia's quest for digital sovereignty*. German Council on Foreign Relations (DGAP). https://dgap.org/sites/default/files/article_pdfs/DGAP-Analyse-2022-01-EN_0.pdf
- European Commission (EC). (2023, October 30). *Commission welcomes G7 leaders' agreement on Guiding Principles and a Code of Conduct on Artificial Intelligence* [Press release]. <https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-g7-leaders-agreement-guiding-principles-and-code-conduct-artificial>
- Gerden, E. (2024, August 29). Russia set to cut research spending by 25%. *Science*. <https://www.science.org/content/article/russia-set-cut-research-spending-25>
- Government of Russia. (n.d.). *AI development*.
- Government of Russia. (2013). *Strategy for the Development of the Electric Power Industry of the Russian Federation*. <http://static.government.ru/media/acts/files/0001201304080048.pdf>
- Government of Russia. (2019). *Energy Security Doctrine of the Russian Federation*. <https://minenergo.gov.ru/ministry/energy-security-doctrine>
- Government of Russia. (2020). *Strategy for Development of the Electronic Industry of the Russian Federation for the Period until 2030*. <http://static.government.ru/media/files/1QkfNDghANiBUNBbXaFBM69Jxd48ePeY.pdf>

- Government of Russia. (2023). Strategy of Development of the Telecommunications Industry of the Russian Federation until 2035. <http://static.government.ru/media/files/Pc7fHuejbNvqv17b0RJNv0RIqTo20IUUV.pdf>
- Inclinent. (2022). *Statistics on the outflow of IT specialists from Russia in 2022*. Retrieved November 20, 2024, from <https://inclinent.ru/outflow-it-specialists>
- Interfax. (2025, September 27). *Russia to spend over 5 bln rubles to support development of AI technology in 2024 – Mishustin*. <https://interfax.com/newsroom/top-stories/94917>
- International Energy Agency (IEA). (n.d.). Energy system of Russia. Retrieved November 20, 2024, from <https://www.iea.org/countries/russia>
- International Telecommunication Union (ITU). (n.d.-a). Russian Federation. Retrieved November 20, 2024, from <https://datahub.itu.int/data/?e=RUS>
- ITU. (n.d.-b). Russian Federation fixed-broadband internet basket. Retrieved April 8, 2025, from <https://datahub.itu.int/data/?e=RUS&c=701&i=34616>
- Kholupova, K. (2024, March 26). Baikal processor localises one of the production stages. *Vedomosti*. <https://www.vedomosti.ru/technology/articles/2024/03/26/1027924-razrabotchik-protssessorov-baikal-lokalizuet-odin-iz-etapov-proizvodstva>
- Kolomychenko, M. (2024). The impact and limits of sanctions on Russia's telecoms industry. *DGAP*. Retrieved June 17, 2025, from <https://dgap.org/en/research/publications/impact-and-limits-sanctions-russias-telecoms-industry>
- Kommersant. (2023, April 14). Woe from wit: The use of AI to be regulated by law. <https://www.kommersant.ru/doc/5928661>
- Kommersant. (2024, April 9). Law abiding intelligence. <https://www.kommersant.ru/doc/6621034>
- Kurasheva, A. (2023, July 28). Foreign companies still hold 30% of the Russian cybersecurity market. *Vedomosti*. <https://www.vedomosti.ru/technology/articles/2023/07/28/987508-zarubezhnie-zanimayut-30>
- Miller, A. (2024, September 30). Russia to allocate a record 13.5 trillion rubles for war in 2025. *DW*. <https://www.dw.com/ru/rossia-vydelit-v-2025-godu-na-voynu-rekordnye-135-trln-rublej/a-70368182>
- Nadibaidze, A. (2022). *Russian perceptions of military AI, automation, and autonomy*. Foreign Policy Research Institute (FPRI). <https://www.fpri.org/wp-content/uploads/2022/01/012622-russia-ai-.pdf>
- National Archives. (n.d.). *Global war on terror*. Retrieved November 20, 2024, from <https://www.georgewbushlibrary.gov/research/topic-guides/global-war-terror>
- Norem, J. (2024, April 22). *Russia is working on a 128-core supercomputing platform: Report*. ExtremeTech. <https://www.extremetech.com/computing/russia-is-working-on-a-128-core-supercomputing-platform-report>
- Organisation for Economic Co-operation and Development (OECD). (2023). *OECD science, technology and innovation outlook 2023*. https://www.oecd.org/en/publications/oecd-science-technology-and-innovation-outlook-2023_0b55736e-en.html
- OECD. (2024). *New perspectives on measuring cybersecurity*. https://www.oecd.org/en/publications/new-perspectives-on-measuring-cybersecurity_b1e31997-en.html
- Petrella, S., Miller, C., & Cooper, B. (2021). Russia's artificial intelligence strategy: The role of state-owned firms. *Orbis*, 65(1), 75–100. <https://doi.org/10.1016/j.orbis.2020.11.004>
- Pfaff, C. A. (Ed.). (2025). *The weaponization of AI: The next stage of terrorism and warfare*. Centre for Excellence Defence Against Terrorism (COE-DAT). <https://www.tmmm.tsk.tr/publication/researches/21-TheWeaponizationofAI-TheNextStageofTerrorismandWarfare.pdf>
- President of Russia. (2016). Decree of the President of the Russian Federation No. 646 dated 5 December 2016 on the Approval of the Information Security Doctrine of the Russian Federation. <http://www.kremlin.ru/acts/bank/41460>
- President of Russia. (2019a). Decree of the President of the Russian Federation No. 216 dated 13 May 2019 on the Approval of the Energy Security Doctrine of the Russian Federation. <http://static.kremlin.ru/media/events/files/ru/rsskwUHzl25X6lijBy20Doj88faOQLN4.pdf>
- President of Russia. (2019b). Decree of the President of the Russian Federation No. 490 dated 10 October 2019 on the Development of Artificial Intelligence in the Russian Federation. <http://www.kremlin.ru/acts/bank/44731>
- President of Russia. (2021). National Security Strategy of the Russian Federation. <http://www.scrf.gov.ru/media/files/file/l4wGRPQJvETSkUTYmhepzRochb1j1jqh.pdf>
- President of Russia. (2024). Decree of the President of the Russian Federation No. 124 dated 15 February 2024 on Amendments to the Decree of the President of the Russian Federation No. 490 dated 10 October 2019 on the Development of Artificial Intelligence in the Russian Federation. <http://publication.pravo.gov.ru/document/0001202402150063>

- RBC. (2022, May 28). *Experts assess the impact of IT specialists towards the end of the last half year*. https://www.rbc.ru/technology_and_media/28/05/2022/628fa85d9a7947dabe3b3e30
- Realnoye Vremya. (2024, August 4). Over the past two years, the drain of IT specialists in Russia has decreased. <https://realnoevremya.ru/news/314247-v-rossii-uluchshilas-obstanovka-otnositelno-otezda-it-specialistov>
- Ross, S. (2024, August 28). *The 5 biggest Russian banks*. Investopedia. Retrieved November 20, 2024, from <https://www.investopedia.com/articles/investing/082015/6-biggest-russian-banks.asp>
- Russian Federation. (2006). Federal Law on Personal Data (as amended as of 8 August 2024). <https://docs.cntd.ru/document/901990046>
- Rutland, P. (2008). Russia as an energy superpower. *New Political Economy*, 13(2), 203–210. <https://prutland.faculty.wesleyan.edu/files/2015/08/Russia-as-an-energy-superpower.pdf>
- Sidelnikova, D. (2024, February 27). *Three more Yandex services have been included in the register of user tracking. What does this mean and how can you protect yourself?* Takie Dela. <https://takiedela.ru/notes/utechka-dannykh/>
- SimilarWeb. (2021). *Top websites ranking*. Retrieved November 20, 2024, from <https://www.similarweb.com/top-websites/russian-federation/computers-electronics-and-technology/social-networks-and-online-communities/>
- Starchak, M. (2024, August 16). *Russian defense plan kicks off separate AI development push*. DefenseNews. <https://www.defensenews.com/global/europe/2024/08/16/russian-defense-plan-kicks-off-separate-ai-development-push/>
- Statista. (2024). *Leading countries by gross research and development (R&D) expenditure worldwide in 2022*. Retrieved November 20, 2024, from <https://www.statista.com/statistics/732247/worldwide-research-and-development-gross-expenditure-top-countries/>
- Stix, C. (2022) Foundations for the future: Institution building for the purpose of artificial intelligence governance. *AI Ethics*, 2, 463–476. <https://doi.org/10.1007/s43681-021-00093-w>
- TAdviser. (2025). *390 billion rubles of investment and 2,000 AI developers: The Ministry of Economic Development summed up the results of the federal project "Artificial Intelligence"*. Retrieved April 8, 2025, from <https://shorturl.at/z1NBm>
- Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M., & Lundgren, M. (2023). The global governance of artificial intelligence: Next steps for empirical and normative research. *International Studies Review*, 25(3). <https://academic.oup.com/isr/article/25/3/viad040/7259354>
- TASS. (2024, July 8). *AI developers will insure against risks for potential harm to life from technology*. <https://tass.ru/obschestvo/21307449>
- Telecom Daily. (2024). *Programmer attrition has ceased to be a problem for Russian IT companies*. Retrieved November 20, 2024, from <https://shorturl.at/utQNw>
- Tencent. (2024). *Corporate overview*. Retrieved November 20, 2024, from <https://static.www.tencent.com/uploads/2024/08/14/20913f7ba15aacb47b51d502f1cc1da4.pdf>
- TOP500. (n.d.). *The list*. Retrieved April 8, 2025, from <https://top500.org>
- Tyunyaeva, M. (2023, December 14). What AI threats did Vladimir Putin warn about? *Vedomosti*. <https://www.vedomosti.ru/technology/articles/2023/12/14/1011153-ugrozah-ii-putin>
- UN Interregional Crime and Justice Research Institute (UNICRI) & UN Office of Counter-Terrorism (UNOCT). (2021a). *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes*. <https://unicri.org/News/Algorithms-Terrorism-UNICRI-UNOCCT>
- UNICRI & UNOCT. (2021b). *Countering terrorism online with artificial intelligence*. <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf>
- Ünver, H. A. (2024). *Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights*. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA\(2024\)754450_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2024/754450/EXPO_IDA(2024)754450_EN.pdf)
- Urusov, P. (2023, July 25). *Vital microchip sanctions will hit Russian computing power hard*. Carnegie Politika. <https://carnegieendowment.org/russia-eurasia/politika/2023/07/vital-microchip-sanctions-will-hit-russian-computing-power-hard?lang=en>
- US Department of the Treasury. (2024). *Managing artificial intelligence-specific cybersecurity risks in the financial services sector*. <https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf>
- Zinovieva, E. (2024, October 31). *What's wrong with the Global Digital Compact?* Russian Foreign Affairs Council. <https://russiancouncil.ru/analytics-and-comments/analytics/chto-ne-tak-s-globalnym-tsifrovym-dogovorom>

Annexure: KASE mapping tool

General questions	KASE dimensions	KASE dimension-specific questions
<p>1. Is there a strategy? If so, which public entity (e.g., ministry) defines and implements it?</p> <p>2. Is there any regulation? If so, which public entity (e.g., regulatory authority) oversees regulating?</p> <p>3. Is there a funding mechanism stimulating R&D and innovation? If so, which entities orchestrate the funding mechanism? Which mechanisms exist to incentivise innovation?</p> <p>4. Which are the key private-sector or non-governmental stakeholders (e.g. national champion(s), dominant actors, or non-governmental bodies)? Which are their main interests (provide examples)? Is there any foreign private entity with particular relevance in the sector?</p> <p>5. Is there a strategy of international cooperation or expansion of national sector?</p>	Data (personal, non-personal, critical, confidential, etc.)	<p>1. How is the country's census infrastructure in terms of capacity and diversity?</p> <p>2. Are high-quality, diverse data sets easily available?</p> <p>3. Are there AI-ready datasets?</p> <p>4. Is there a strategy for data commons?</p>
	Algorithms (including models, etc.)	<p>1. Is there any policy for open-source software development?</p> <p>2. Does the public administration use proprietary software developed domestically or by foreign players, or open software?</p> <p>3. What are the AI procurement rules, if any?</p> <p>4. Is there any public-private partnership mechanism to incentivise development and deployment of algorithms?</p>
	Computing capacity value chain (including servers, storage resources, etc.)	<p>1. Which kind of public computing capacity is there?</p> <p>2. Are there public supercomputers?</p> <p>3. What is the largest computing cluster?</p> <p>4. Are they available for private sector use?</p> <p>5. Are there any components manufactured in the country?</p> <p>6. What are the most notable investments in the various elements of the computing capacity value chain?</p> <p>7. Is there a strategy for capacity building for cutting-edge work in the computation supply chain?</p>
	Connectivity infrastructure (including submarine cable, terrestrial, and satellite infrastructure)	<p>1. How meaningful is connectivity (affordability, zero-rating in place, proportion of access by type of device, by gender, by economic segment, etc.)?</p>
	Electricity infrastructure (including renewables and batteries, etc.)	<p>1. Is there a stable, reliable, and affordable electrical power supply throughout the country?</p> <p>2. Are there relevant discrepancies within the country in terms of energy supply and infrastructure?</p> <p>3. What is the proportion of electricity produced via renewable sources?</p> <p>4. Is there any regulation for the use of electricity for specific types of technology?</p>
	Education, talent promotion, and retention	<p>1. What is the digital literacy rate?</p> <p>2. How many computer scientists and engineers graduate per year?</p> <p>3. Are there specific degrees (Bachelor's and Master's) specifically targeting AI from public universities?</p> <p>4. Is there any public initiative to foster AI studies?</p> <p>5. Are there specific courses or certifications for AI for public servants?</p> <p>6. Is it within the public administration?</p> <p>7. What are the immigration patterns of AI scientists?</p> <p>8. Is the country importing or exporting AI talent?</p>
	Cybersecurity	<p>1. Are there specific protection policies for AI-related infrastructure (such as supercomputers)?</p> <p>2. Is there a public body fostering coordination among agencies and public administration with competences on cybersecurity?</p>
	Digital public infrastructure (DPI) (DPI for AI, and AI for DPI)	<p>1. Is there a definition of DPI?</p> <p>2. Are there AI components within major DPIs (digital ID, payment methods, data sharing platforms)?</p> <p>3. Is AI used in other public software platforms that could be considered DPIs?</p> <p>4. Are there specific AI software and hardware labelled as DPI?</p> <p>5. Has the government developed or promoted the development of any generative LLM?</p>

Source: CyberBRICS (n.d.)