

THE POWER OF CAPITAL IN TIMES OF WAR

THE CASE OF ICT FIRMS IN RUSSIA

By

Anastasiia Ptichkina

Submitted to Central European University – Private University

Department of Political Science

In partial fulfillment of the requirements for the degree of Master of Arts in Political Science

Supervisor: Professor Inna Melnykovska

Vienna, Austria

2025

Copyright Notice

Copyright © Anastasiia Ptichkina, 2025. The Power of Capital in Times of War: The Case of ICT Firms in Russia – This work is licensed under [Creative Commons Attribution-NonCommercial-ShareAlike \(CC BY-NC-ND\) 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/) International license.



For bibliographic and reference purposes this thesis/dissertation should be referred to as:
Ptichkina, Anastasiia. 2025. The Power of Capital in Times of War: The Case of ICT Firms in Russia. MA thesis, Department of Political Science, Central European University, Vienna.

¹ Icon by [Creative Commons](https://creativecommons.org/)

Author's declaration

I, the undersigned, **Anastasiia Ptichkina**, candidate for the MA degree in Political Science declare herewith that the present thesis is exclusively my own work, based on my research and only such external information as properly credited in notes and bibliography. I declare that no unidentified and illegitimate use was made of the work of others, and no part of the thesis infringes on any person's or institution's copyright.

I also declare that no part of the thesis has been submitted in this form to any other institution of higher education for an academic degree.

Vienna, 4th of June 2025

Anastasiia Ptichkina

Abstract

After the outbreak of full-scale war with Ukraine on February 24, 2022, Russian IT sector found itself both the most protected and the most vulnerable positions. While the state introduced sweeping incentives for accredited IT companies – such as military draft deferments, tax breaks, and subsidies for import substitution – it simultaneously employed punitive tools including the revocation of accreditation, forced ownership changes, and exclusion from strategic markets. The analysis draws on theoretical frameworks of crony capitalism, structural and organizational power, and more. Using case studies of firms with varying capital, this thesis examines the interplay between firm behavior and state priorities. Findings show that structural and organizational power offer only conditional protection, and that political loyalty increasingly determines access to state patronage.

This research contributes to the understanding of firm-state relations under autocracy, emphasizing the agency of firms in navigating coercive environments, and discussing how selective patronage system works in Russia.

Table of contents

Copyright Notice.....	ii
Author's declaration.....	iii
Abstract.....	iv
List of Tables	vi
Introduction.....	1
Chapter 1. Review of contemporary research.....	8
Digitalization in Illiberal Regimes	8
State-Business Relations in Illiberal Digital Economy.....	11
Chapter 2. Research design.....	15
Key Concepts and Operationalization	15
Hypotheses.....	21
Method	23
Selection of cases.....	24
Chapter 3. Empirical Analysis	26
Institutional Policies Supporting the ICT Sector	26
Institutional Mechanisms of Control and Constraint	28
Selectivity and Room for Maneuver: Insights from Prior Research.....	31
Dynamics of structural power	32
Dynamics of organizational power	34
Political (dis)loyalty of Russian IT-firms	37
Discussion of the results	39
Conclusion	43
Bibliography	46

List of Tables

Table 1. Operationalization of Dependent Variable: State Treatment of IT Firms.....16

Table 2. Operationalization of Independent Variable: Structural and Organizational Powers.....18

Introduction

The Russian invasion of Ukraine on February 24, 2022, was too sudden for the whole world, despite various warnings and speculations in the mass media and in an expert field. The idea that a great war would ever return to Europe seemed unthinkable for many European leaders and citizens, many of whom could still believe in the “end of history” paradigm even if they did not explicitly recognize it as such. But it was also impossible for many Russian citizens to imagine that their state would, for the first time in many years, enter into a full-scale war and end up in an economic and political blockade that would isolate the country's economy from a great part of the world markets. The two significant waves of emigration in February-March and September 2022, following the announcement of “partial mobilization”², indicate that a considerable number of young individuals perceive continued residence and economic participation in Russia as ideologically untenable. PONARS Eurasia provides empirical evidence to the motives of these emigration waves stating that 64% of the interviewees mentioned moral opposition to war as a motive for emigration, and 55% feared future repression (Kamalov et al, 2022). The largest social groups among Russian migrants were IT specialists, and, specifically, employees of Russian IT companies also known as “relocants” (and the term for such immigration was called “relocation”). As a survey conducted by the independent research company OutRush has shown, information technology professionals make up 43% of those who have emigrated from the country. Among them, 80% indicated that they left mainly because of political disagreements with the Russian authorities, whereas just

² “Partial mobilization” refers to the Presidential Decree of 21 September 2022 No. 647 “On the announcement of partial mobilization in the Russian Federation”, which introduced the mobilization of reservists and former military personnel to support Russia’s military operations in Ukraine. Although termed “partial,” the mobilization was marked by legal ambiguity and broad implementation, leading to widespread fear of conscription among young men and professionals.

37% mentioned the risk of mobilization as being among the grounds for emigrating (Kamalov et al, 2025). The number of those who left the country after the announcement of the “partial mobilization” could reach 700,000 people (Forbes, 2025). A significant number of IT professionals and companies have moved to countries such as Georgia, Armenia, Serbia and Turkey.

Comprehensive data detailing the exact proportions of micro, small, medium, and large IT companies in Russia from 2022 to 2025 remains scarce. According to the Federal State Statistics Service (Rosstat) (2024), average number of employees in ICT small enterprises including microenterprises was 197.9, 218.6 209.9 thousand people in 2021, 2022 and 2023 subsequently, and 38.8 42.9 and 46.4 thousand people for medium-sized enterprises. These numbers do not take into account individual entrepreneurs, self-employed, and freelancers (Federal State Statistics Service, 2023). Over 84% (approximately 2.6 trillion rubles) was generated by large and medium-sized enterprises, while small enterprises accounted for nearly 16% (around 0.5 trillion rubles) (Analytical Center under the Government of the Russian Federation, 2024). Most importantly, these numbers indicate that most of the IT workers are employed in small enterprises. There are about 200 thousand SMEs in the Russian IT market, and they occupy a dominant position – about 75% of the total number of enterprises. Of these, 89 thousand are medium-sized companies. And the number of self-employed providing IT services is noticeably high – 750 thousand people (Litvinov, 2024). Although no official statistics clearly distinguish between individual employees, freelancers, and entrepreneurs who relocated from Russia’s IT sector after 2022, it is logical to suppose that micro-entrepreneurs and independent workers had the greatest mobility, while small IT companies with a scattered organization were able to relocate as a company. Large companies could lose individual

specialists but rarely left as whole legal entities. Due to the specifics of the IT profession, they were able to leave as painlessly as possible. For many full-time workers, since the COVID-19 pandemic, the remote work model has become the norm.

As programmers, software engineers, and computer scientists began to leave the country en masse, Russian officials quickly realized that they need to tighten control over the sector. This became particularly evident after whole entities and parts of companies with Russian pedigree started to leave (e.g. JetBrains, Playrix, Prequel, Miro, some former divisions of Yandex like Nebius.AI, Toloka, Avride). At the same time the majority of Western transnational companies also left the market and ceased to provide their IT services, creating an extreme need for substitutes in Russia (The Moscow Times, 2025). In this environment, Russian policymakers turned to a strategy that can best be described as “sticks and carrots”, using both harsh legal instruments against potential dissent and making the IT sector a privileged part of Russian society. The brightest examples of the “privileges” are large tax exemptions and the programs of mortgages for employees of IT-companies which were introduced in the federal laws and approved by the Federal Assembly. What is also important in the context of the war against Ukraine is that IT specialists are eligible for a certain deferral from mobilization in line with Putin’s Decree of March 3rd, 2022 (President of the Russian Federation, 2022).

However, the essence of these policies leaves some room for selective application, which the state actively takes advantage of. Previously described dynamics would lead us to expect, according to the prevailing literature, that the Russian government would turn the IT sector into a permanently guarded industry, granting it wide-ranging support to keep talent and innovative potential in place especially in the wartime and under the sanctions when the need for

substituting technologies is colossal. Empirical developments since the full-scale invasion of Ukraine, however, paint a more ambiguous picture: IT companies constitute a semi-privileged, semi-vulnerable group within this cohort of Russian enterprises. While the state officially proclaimed the IT sector to be strategically privileged and imposed supporting policies like tax exemptions and mobilization deferments, these benefits were distributed unevenly. Some companies were pampered and have enjoyed protective incentives – such as draft deferments and tax relief – while others were excluded from different programs or even targeted by exerting administrative pressure, had their accreditation taken away, faced reputational assault, or been subject to regulatory harassment. Such variation requires explanation.

This pattern reveals a theoretical puzzle of the research. Authoritarian regimes have a tendency to treat high-tech sectors strategically – shielding them from repression in exchange for economic rewards and geopolitical competitiveness (Guriev & Treisman, 2015). The Russian state's early response to the wartime outflow of IT specialists (or so-called "brain drain") seemed to follow this logic, positioning the industry as privileged through public messaging and supporting measures. However, recent events show that state policy has not uniformly been supportive.

Comparative research from other authoritarian settings, most notably Belarus, suggests that IT companies can become targets of selective repression when they are seen as politically disloyal or influence public opinions. During and following the 2020 protests in Belarus, numerous IT companies and digital professionals were singled out and got punished for their alleged support of civil society and protest movements (Freedom House, 2021). These studies suggest that

authoritarian regimes like Lukashenko's may turn against even economically valuable sectors too if they are threatening the political authority.

There are multiple examples of repressions against the sector with unprovoked attacks on entrepreneurs and whole companies (Kravits-Meinke, 2024). At the same time, a lot of initial “privileges” obtained in 2022 are now backtracked: for instance, a large number of IT companies lost the status of “accredited” IT companies which provide all the benefits (CNews, 2024). Among them are Skyeng, Tinkoff Tech, Kontur, Alfa Tech, and several subsidiaries of VK Group, which reportedly failed to meet updated accreditation criteria related to software localization, revenue structure, or personnel relocation. This means that the companies in question immediately lost their tax benefits, and their employees lost their immunity from military conscription. This creates a strategic dilemma for IT companies: allowing employees to relocate often results in the loss of accreditation and government benefits, while meeting government criteria increases political and legal risks. As a result, companies have to choose between safeguarding employee autonomy and securing government support.

Selective enforcement of these policies constitutes the fundamental *research question* of this work: *Why are certain IT companies rewarded while others are excluded or even punished?* How can they navigate in these permanently altering policies and keep their labor force safe and sound, revenues stable and operations sustainable?

In this sense, the IT sector is not a typical or entirely exceptional case – it exists in a twilight zone of the political economy, and the Russian state's unpredictable behavior toward these

firms is particularly interesting. This research focuses on development of the Russian IT industry since February 24, 2022, and considers it a strategically significant yet politically unpredictable sector in the wider authoritarian economic context. Although the IT industry shares several characteristics with other high-tech or export-oriented industries in Russia, there are also some unique aspects that make it an analytically rich case.

Previous studies on authoritarianism have also illuminated in significant ways how regimes use selective repression and incentives as instruments for maintaining control. Much of that research, however, has been focused on the incumbent authoritarian tactics – investigating the ways the state manages opposition, rewards loyalty, or coerces compliance. Although these papers have assisted me in reconstructing the image of how modern autocracies operate, they underestimate the strategic agency of private actors. Though such newer approaches are useful for tracing the logic of state action, they do not cover the strategic agency of private firms and what is driving their choices.

So, this study shifts the focus to the firms themselves. And, by aiming at the ways in which firms navigate the politics, adapt or resist co-optation, and align themselves according to changing state imperatives, this study adds a bottom-up dynamic to the study of authoritarian governance. By doing so, it seeks to contribute to the literature by placing the firms not simply as passive takers of state policies, but as actors that can influence the terms under which they are treated. This study explores how IT firms' behavior and status shape the type of treatment that IT firms receive from the Russian state, i.e., selective repression (or “sticks”) or policy of rewards/benefits (“carrots”) and what conditions make some firms more receptive to punishment or more prone to obtaining access to benefits. This study contributes to the

literature on authoritarian political economy by examining how state support is distributed unevenly across strategic sectors, using the Russian IT industry as a case study. It engages with debates on authoritarian responsiveness, selective policy implementation, and the role of informal institutions in shaping economic governance in the context of the great war.

The structure of the thesis is as follows: Chapter 1 introduces the overview of theoretical approaches to digitalization in illiberal regimes and to state-business relations in illiberal digital economy. It outlines the principal models – competitive authoritarianism, informational autocracy, crony capitalism and their relative strengths and weaknesses in explaining selective treatment of Russian IT firms. Particular attention is paid to the concept of organizational and structural power, preparing background for the thesis' framework. how these models handle (or fail to handle) firm agency. Chapter 2 sets out the research design, case selection, and operationalization of dependent and other variables of interest. Three main hypotheses and sub-hypotheses are also presented in this section. Chapter 3 is dedicated to testing the introduced hypotheses and presents empirical evidence from a comparative study of IT companies, presenting unexpected results. Finally, the study of Russian IT firms is concluded and in this chapter perspectives for future research are proposed.

Chapter 1. Review of contemporary research

When talking about Russian IT firms, it is crucial to understand the context in which they operate, and most importantly, what approaches for studying the specifics of the Russian developing economy exist in the literature. In this subsection I will focus on the existing approaches to decide whether they have the potential to become helpful to obtain the knowledge of how one firm is treated by the Russian government based on its background, actions and other crucial characteristics.

Digitalization in Illiberal Regimes

In Levitsky and Way's (2010) foundational work on competitive authoritarianism modern to their day Russia was characterized as a country with a hybrid regime, where democratic institutions do exist but consistently are manipulated by incumbents for the purpose of staying in power. These regimes combine democratic features such as elections, opposition parties, and independent media with authoritarian practices – e.g.: electoral and judicial manipulation, repression of opposition. This research is relevant to the study of state-business relations in the Russian IT industry, while the Kremlin used selective legal and political coercion to achieve corporate compliance while maintaining the institutions of market competition and legality. Levitsky and Way point out how political protection and access to state resources are traded for political loyalty. They describe how such regimes regulate elite competition and institutional uncertainty in a way to preserve authoritarian rule without exposing the system as not truly democratic. However, after the outbreak of full-scale war in Ukraine, or even in the earlier years, Russia moved away from hybrid tactics toward more openly coercive and

militarized governance. The model assumes a level of pluralism that no longer exists in post-2022 Russia, hence, this model is not fully eligible for studying how “carrots and sticks” are distributed.

The following framework could be useful for analyzing privilege and informal ties. The crony capitalism framework, developed by George M. Taber in 1980 to describe political favoritism under the Marcos rule in the Philippines, was later solidified as a formal analytical model by Stephen Haber. In *Crony Capitalism and Economic Growth in Latin America: Theory and Evidence* (2002), Haber conceptualizes crony capitalism as a system where economic resources (e.g. credit, licenses, and state contracts) are not allocated based on efficiency or competition, but through informal political connections. Similarly, Kang (2002), in their study of South Korea, demonstrates how the state’s reliance on business loyalty overrule-based regulation drove rapid growth (The Miracle on the Han River) but rooted corruption and economic vulnerability which are visible up to our days. These works explain how authoritarian regimes gather elite support and economic control through selective privileges.

Specifically, Anders Aslund’s “Russia’s Crony Capitalism” (2019) provide account on full-scale kleptocracy, where state power and private wealth are tightly interlinked. This framework is useful for addressing the puzzle of selective state treatment of IT firms: access to state benefits often reflects political alignment rather than innovation or market value. However, classic crony capitalism literature assumes too simplistic logic where loyal firms are rewarded, disloyal ones excluded. The behavior of Russian IT companies should be at least viewed as bit more complex. Many firms pursue specific strategies: partially complying with state expectations while preserving autonomy through relocation, dual market strategies, or

institutional compartmentalization. Therefore, while the crony capitalism model offers a solid foundation for explaining resource allocation under authoritarianism, it requires to be complemented with frameworks that account for firm agency and adaptive behavior.

Another researcher Simeon Djankov (2015) argues that the Russian economy under Vladimir Putin has shifted from classical crony capitalism to a model of state capitalism, where the state or its proxies acquire strategic assets in order to ensure political loyalty. This centralization allows the Kremlin to distribute resources and suppress competition, aligning economic power with state interests. Though this model assists in understanding how selective support is organized from the top, it ignores the agency of companies, particularly those in strategic industries such as IT, where firms tend to adapt by hedging between state compliance and international integration.

Finally, Frye (2010) emphasizes the continued role of informal institutions and weak rule of law in shaping the post-Soviet business environment. In the context of the Russian IT sector, this insight helps explain the coexistence of innovation with political vulnerability. Frye argues that in states with polarized democratic institutions and inconsistent legal enforcement, firms are more likely to rely on political connections than on formal guarantees of property rights, just as it is like in crony capitalism. Applied to Russian IT companies, this suggests that their growth and protection often depend less on legal frameworks than on their relationship to the state. Companies closely aligned with state interests may receive preferential treatment, while others remain exposed to arbitrary enforcement, selective repression, or exclusion from benefits – especially in times of political turbulence. This dynamic creates a fragmented and uncertain business landscape where technological entrepreneurship is shaped not only by

market logic but also by political expediency. However, this study does not offer tools to distinguish why some firms are punished while others are rewarded within the same institutional environment.

State-Business Relations in Illiberal Digital Economy

The state and business relations in the context of Russian digital autocracy has also been a subject of studies of Guriev and Treisman (2015). Their theory of informational autocracy provides a more flexible framework. The authors argue that such regimes survive not through mass repression alone but through a combination of cooptation, selective censorship, and propaganda. Such mechanisms allow the dictators to remain in power while minimizing public resentment and external criticism. The authors introduce the term “informational autocracy” – regime where governments manipulate the informational environment to appear legitimate and competent, and thus they do not need to use brute force to suppress opposition. Repression, when used, is often selective and directed at individuals or groups that challenge the regime’s narrative or organizational control. This model explains why countries with authoritarian regimes, like Russia, invest heavily in media control, internet surveillance, and forming valuable alliances, especially with the information technology industry. However, this framework may also no longer fully apply to contemporary Russia following the fundamental transformations that began with the outbreak of Russo-Ukrainian war. Prior to the COVID-19 pandemic and before February 24, 2022, limited freedom of speech persisted in some media outlets. In the current context, however, independent media and political opposition have been systematically labeled as foreign agents, extremist and terrorist organizations, and their activities on the territory of the Russian Federation are no longer possible.

The next approach allows mapping selective “carrots and sticks” onto real firms. Gerschewski (2013) offers a broader perspective through his three pillars of authoritarian stability: legitimization, repression, and co-optation as essential for the stability of autocratic regimes and describes how they influence market dynamics. His “three pillars” framework, though designed to study political regimes, provides unintended insights into the interplay between state and business actors in hybrid economies like Russia’s. Legitimation relies on ideological narratives or performative actions to cultivate public approval. Repression employs threats or force to suppress opposition, while co-optation secures elite loyalty by integrating them into the regime’s power structures. Gerschewski argues that these pillars are interdependent and reinforce one another: effective co-optation reduces the need for repression, and legitimization can facilitate both co-optation and compliance. The survival of an autocracy therefore depends on the regime’s ability to balance and institutionalize these mechanisms over time. This framework provides a useful analytic tool for considering the ways in which authoritarian regimes, like Russia, manage the complex interplay between control and consent in sectors like IT. For instance, the co-optation pillar, manifested through state-corporate partnerships or selective subsidies, may explain how certain IT firms thrive while others face constraints. In relation to the research puzzle of the current work, it could be applied in the way that co-optation pillar is crucial for understanding why some firms get “sticks”, while others gain “carrots”.

Tsai (2007) develops the concept of adaptive informal institutions which offers a valuable perspective on how actors navigate authoritarian systems by creating parallel practices that achieve official goals while subverting formal rules. Originally developed to explain local innovation under China’s centralized governance, this framework emphasizes how

organizations adapt by aligning with state expectations while pursuing their own interests beneath the surface. The study analyzes how local officials and economic actors in China's authoritarian system adapt to rigid formal requirements from above by creating informal practices that are outwardly compliant with instructions but also allow them to solve practical problems and achieve autonomy. These adaptive informal institutions emerge when formal rules are unsustainable, but it is risky to formally violate them. For example, officials lacking sufficient funding from the center may come up with workarounds, formally complying with orders but de facto distorting their implementation to meet party demands and the real local needs.

In the context of the Russian IT sector, this approach helps explain the behavior of those companies that formally comply with government requirements (e.g., inclusion in registries, declarative support), but actually act autonomously: they transfer personnel abroad, split the ownership structure, continue cooperation with foreign partners, or operate in the gray zone. In the context of Russian IT firms, this lens helps explain how companies may appear compliant – for example, by registering software locally or avoiding public criticism of the regime, while quietly relocating staff, diversifying ownership, or shifting parts of their operations abroad. Unlike traditional crony capitalism models, which assume passivity or full loyalty, Tsai's framework captures the strategic creativity of firms operating under constraints. It complements Gerschewski's emphasis on regime tools (repression, co-optation) by foregrounding how targeted firms respond, maneuver, and resist without outright defiance.

And finally, beyond political loyalty, some firms may be shielded from repression or granted privileges based on their position in the economic and institutional hierarchy. This logic reflects

the classic distinction between *structural* and *organizational power*. As Susan Strange (2015) argued, governments are structurally dependent on private investment and thus, firms shape state behavior indirectly. In the Russian context, Sber and VK businesses are not necessarily required to manifest loyalty since their removal would be disruptive to state activities. Organizational power, on the other hand, is an internal capacity to comply, adapt, or build connections. It has four aspects: security, knowledge, production, and finance. Michael Mann (1984, p. 189) refers to this as “*the infrastructural power of the state – the institutional capacity to penetrate and coordinate social life*”, a concept that can be applied to firms embedded in bureaucratic systems such as Skolkovo. These two forms of power provide a basis for explaining why some firms are treated more cautiously or favorably than others.

Chapter 2. Research design

Key Concepts and Operationalization

Attempts of Russian state to control the IT sector are quite sporadic. Despite this, three years after the beginning of the full-scale war, some trends can already be analyzed. Russian politics in regards of IT sector is not coherent and sometimes can take the form of sanctions and punishments, while at other times they concentrate on providing bonuses and privileges to the sector. Building on this idea, the research question focuses on identifying the factors that explain why certain IT companies receive repressive or supportive treatment from the Russian government. In this design, the *dependent variable (DV)* is the policy outcome experienced by a company – ranging from political pressure (e.g., defamation in state media, legal prosecution, or other forms of repression and positive punishment) to state support or certain incentives (e.g., tax exemptions, access to public tenders, or mobilization deferment for IT-specialists). This includes both the level of privileges granted and the company's continued eligibility for government support programs. The study aims to understand what characteristics or behaviors of companies – such as ownership structure, political alignment, relocation decisions, or market prominence – shape their treatment by the state. In case of the Russian Federation, uncovering the exact motivations behind political choices is particularly challenging, if not impossible. However, a comparative perspective allows for an analysis of how the government's approach to different IT companies and industry as a whole differs depending on what is currently profitable to the state. And, most importantly, specific IT companies, including micro-enterprises, as well as teams and individual entrepreneurs, whose strategies of interaction with the state range from cooperation to distancing and relocation, are considered as the unit of analysis.

Table 1. Operationalization of Dependent Variable: State Treatment of IT Firms

Type of State Treatment	Operational Indicators	Explanation
Repression (“Sticks”)	Legal/administrative pressure or positive punishment (e.g., fines, tax inspections, “foreign agent” designation)	Used to signal noncompliance and apply institutional costs to autonomous firms
	Blocking or restricting access to websites/services in Russia	Limits firm's market access or public visibility
	Public prosecution or defamation of management	Targets firm leadership to deter dissent or promote compliance
	Negative punishment (e.g., excluding a firm from subsidies, tenders, or official recognition).	Withholding benefits cuts off financial support and market opportunities
	State acquisition of shares or appointment of loyal executives	Enables soft co-optation, thereby bringing them firmly under government objectives
	Forced divestiture, takeover, or nationalization	Applies to strategically important but insufficiently loyal firms.
Support (“Carrots”)	Eligibility for army deferment for employees	Incentivizes compliance by protecting staff from mobilization in the military
	Access to state tenders and subsidies	Provides financial and strategic advantages
	Reduced taxes and regulatory burden	Rewards political alignment through fiscal incentives
	Entrance to state-backed clusters (e.g., Skolkovo, Innopolis)	Institutionalizes privileged status through infrastructure and partnerships

In order to research the differentiated state treatment of Russian IT business since February 24, 2022, it would be better to categorize them according to the level of state impact. By doing this, the study could examine how sticks and carrots are distributed between firms with different types of power (organizational and structural). Hypotheses which are going to be tested in this research rely on this classification; thus, it is crucial to operationalize two concepts. To begin with, there is the cluster of firms that obtain big *structural power* – they are

“too huge to repress” or “too embedded to ignore”. A firm is considered to have high structural power if it remains embedded in critical state infrastructure, maintains exclusive or large-scale government contracts, provides irreplaceable technological services, or contributes directly to state-led initiatives (e.g., domestic cloud services, data hosting, or digital ID systems), as Table 2 suggests. This dynamic is particularly evident in sectors critical to the Russian economy, such as energy, and defense (Matveev, 2019). I assume that VK, Rostelecom, and Yandex (particularly following its 2022 restructuring) belong to this group just like Sber's digital ecosystems: they are so integrated into public services and therefore too politically significant to be shut down. Some Russian IT firms experienced a loss in their structural power after February 24, 2022, that could result from the relocation of key operations or personnel abroad, withdrawal from state procurement platforms, or loss of access to essential technologies due to international sanctions. As the following analysis shows, companies can quickly fall into disfavor once their utility to the regime diminishes. In contrast, firms that retained or increased their structural embeddedness tend to benefit from selective incentives.

A legally secured firm's strategic and systemic importance can also reflect the strength of its structural power. the Ministry of Digital Development, Communications and Mass Media of the Russian Federation regularly updates the “List of backbone organizations of the Russian economy engaged in economic activities in the sectors of the economy, the implementation of state policy” (Ministry of Digital Development, Communications and Mass Media of the Russian Federation, n.d.). The objects of critical infrastructure, established by Federal Law No. 187-FZ, are also the carriers of this structural power (Russian Federation, 2017).

The second big group of firms has big *organizational power* – at least, structurally they are non-essential, but institutionally they are highly embedded. Businesses situated in government-backed IT clusters of innovation or technoparks, like Innopolis and Skolkovo, belong to this category: they have been created and exist directly through federal programs. Inclusion in the Digital Economy national project, or the “Technological Sovereignty” roadmap (known as the “Concept of Technological Development”) also makes a criterion for falling into this category, as well as privileged access to state contracts.

Table 2. Operationalization of Independent Variable: Structural and Organizational Powers

Type of power	Operational Indicators	Explanation
Structural	Dominating positions in the IT market	Set industry standards or control critical infrastructure, making them indispensable to market functioning
	Significant market shares	Reflects economic weight and reduces the cost of state alignment
	Maintains exclusive or large-scale government contracts or contributes directly to state-led initiatives	Goszakupki” for e.g., domestic cloud services and OS, data hosting, or digital ID systems
	Inclusion in strategic and systemic importance registers	Formal recognition by state bodies (e.g., by MinTsifry, in “KII”) as critical to the economy or security, granting access to subsidies and protection.
	Fits in the niche of substitute of the sanctioned goods and technologies	Proves to be an important and irreplaceable player in the context of exodus of foreign companies and technologies
Organizational	Participation in government-backed clusters (e.g., Skolkovo, Innopolis)	Belonging to infrastructures created or supported by the state and financial dependence on them

	Links to state-affiliated elites (e.g., former officials, affiliated owners)	Connections with elites can provide access to informal support, loyalty, or protection from repression
	Inclusion in public procurement and tenders	Signals institutional embeddedness and formal channels of direct communication with the state
	Formal role in national/regional digitalization programs	Though not necessarily productive and active participator

However, it is crucial for the analysis to bear in mind the fact that within the framework of crony capitalism the distinction between organizational and structural power often becomes analytically ambiguous since the boundary could be very blurred: corporation like Sber is majority-owned by the Russian government and plays a central role in implementing national economic projects, what makes it an entity with extremely high organizational power. At the same time, it is the largest bank and tech company – its operations underpin the functioning of the national banking system, including dominance in payment processing and acquiring markets. Its powers are interlinked; organizational power has been strengthening the structural one for decades after the fall of the Soviet Union and even before that (Sber originates to established in 1841 under Tsar Nicolas I “Sberegatelnaya Kassa”). This analysis distances from proposing rigid thresholds – such as specific state ownership shares, board composition criteria, or revenue structures to dichotomize firms into purely organizational or structural power categories. There is simply no such in the literature, what could become a fertile avenue for future research. Thus, in this study, corporate power is operationalized more as a two-dimensional continuum rather than a binary classification. This will be additionally illustrated at the Hypotheses sub-section.

A final and analytically important category consists of firms that possess neither structural nor organizational power. Since they resist co-optation (this is especially true for companies after the outbreak of a full-scale war), they can no longer play a significant role in the local market. Prior to the war, they could be well embedded but then lose everything. Their exclusion from both structural dependence and institutional incorporation makes them more susceptible to selective repression, the state restricts their legal presence through administrative exclusion, reputational targeting, or blanket restrictions on “foreign agents” or “undesirable organizations”. These differences allow us to make sense of the logic of selective incentives and selective repression used by the Russian state: *benefits and protection are offered to the co-operators, while firms opposing the logic of co-optation may be denied supportive policies, subjected to reputational damage, or even legal pressure.*

In this research, there are two independent variables – organizational and structural powers which are conceptualized as firm-level characteristics that shape state response but are not caused by it. They are exogenous to the state immediate policy reaction in the form of sticks or carrots. A firm’s loyalty serves as a moderating variable that alters the relationship between a state’s policy response and the firm’s powers (regardless of what power dominates, they can also be mixed). A firm’s loyalty links both to its proclaimed signaling and behavioral facts – from remaining registered and active in Russia after 2022 to willingness to comply with more and more of new restricting policies regarding accreditation, laws on data storage and software or participation in state-backed programs like “Digital Economy”.

Hypotheses

The government's own stance toward the IT sector shifted under the pressure of external shocks. In the first few months after the invasion, the IT sector was effectively treated as a strategically privileged sphere, with extensive government support against “brain drain” and sanctions. However, as the outflow of companies gained momentum and Russia's financial and administrative resources came under pressure and declined, criteria for this privileged status seemed to have become stricter. The first hypothesis (H1) thus reads:

H1: a firm that has structural power, has state support (e.g., tax breaks, payment deferrals, preferential accreditation).

H1a: a firm that loses structural power (e.g., due to factors such as relocation or technological obsolescence) faces a risk of exclusion from state support mechanisms.

H1b: a firm that has gained structural power post-2022 (e.g., through import substitution of sanctioned technologies) secures state support, even when it lacked prior institutional favor.

The second group of hypotheses concerns the relative influence of IT companies, specifically their institutional embeddedness.

H2: a firm that has organizational power (e.g., participation in state-affiliated clusters, privileged procurement access, or politically loyal management) is shielded from repressive measures and maintains access to state-provided benefits.

H2a: a firm that loses organizational power (e.g. through relocation, ownership changes, or public divergence from state agendas) faces withdrawal of state support and previously granted incentives.

H2b: a firm that gains organizational power (e.g., through governmental policies of import substitution) receives state support and new rewards.

Building on selective incentives and repression theory (Guriev & Treisman, 2015), the study suggests that the Kremlin policy of co-opting private information technology firms didn't start in 2022 but has profound origins in the state's consistent efforts to apply political control on the internet and technology. With this understanding, those firms that declined to align with the state agenda – denying partnership with the government, declining requests for content moderation, or relocating operations overseas – were less likely to be rewarded institutionally through tax breaks, access to tenders, or army deferment for employees. The third hypothesis (H3) is therefore:

H3: A firm that failed to adhere to political loyalty could be shut out from favorable government policies and become an object of repressive treatment after the outbreak of full-scale war regardless of strength of their prior organizational ties and structural power.

Method

Designing a research framework for this kind of study is not a straightforward task. Studies of the factors of government approaches to certain problems and the results of policies are often quantitative. However, in the case of current Russian policy, this may be far from the best choice. The war in Ukraine and the imposition of international sanctions remain ongoing, and the political landscape continues to evolve rapidly. In authoritarian regimes, official data – especially data directly reflecting sensitive matters – can be unreliable. For example, metrics that are typically considered straightforward, such as COVID-19 death rates, may be misrepresented or concealed. Furthermore, a quantitative study may offer limited insight, as its findings risk being quickly outdated or contradicted by subsequent events. Interviews as a method are also not suitable, because to have a conversation with representatives of compliant firms for such a study is a task close to impossible. Given these limitations, this study adopts a comparative case study as the primary method. This qualitative method enables a deeper examination of the relations between the state, federal subjects, and selected IT companies. It will also allow us to build a coherent picture of how the policies towards the IT sector in Russia unfolded in the last three years.

The time frame of the study covers the period from February 2022 – the beginning of the active phase of the war and subsequent mobilization, including “partial mobilization” in September

2022 – to the present, i.e. the first half of 2025. This timeframe allows us to trace key changes in government policy aimed at regulating the IT sector in the context of ongoing conflict and foreign policy pressure. The time frame witnesses significant government policy shifts to respond to wartime needs, sanctions, emigration waves, and internal administrative pressures. The timeframe allows for the observation of both the immediate response (IT specialist protection, support packages) and the following gradual removal of privileges for less-aligned actors.

Selection of cases

In 2024, Russia continues to hold the title as the most sanctioned country globally. A unique case when a large modern state involved in international exchange and cooperation finds itself subject to multilateral sanctions. Economic studies often focus on assessing the damage to the Russian economy from the withdrawal of foreign companies from the Russian market, but rarely do researchers look at the withdrawal of Russian companies from the Russian market and the conditions for their continued operation in the Russian Federation. In addressing this gap, the present study not only focuses on relevant government policies, but also seeks to define specific IT companies, state agencies, and policymakers. The sector is characterized by a high degree of fragmentation and flexibility, which makes it particularly sensitive to public policies and particularly interesting for studying mechanisms of selective repression and incentives.

Measures to support the industry are mainly established by federal laws and resolutions of the Russian government, which indicates that the regions of the Russian Federation do not have sufficient autonomy in making such decisions. Consequently, the assumption of significant

regional variation in support measures does not hold, as there is no legal framework for the existence of such differentiation. Rather than regional discrepancy, the landscape is characterized by federally initiated projects, such as innovation clusters like Skolkovo of Moscow region and Innopolis of the Republic of Tatarstan, which however, were launched prior to the beginning of the war and deployment of discussed sanctions (Kuleshova, 2020).

Analysis covers only cases where at least one type of power is present. There is a category of firms which lack both organizational and structural powers - the fourth, and subsequently the forth hypothesis could be introduced, however, it does not fall into focus of the current research since the powers constitute independent variables of the proposed model. The analysis is based on reasonable but partially extrapolated assumptions, drawing on public sources, news outlets and industry interviews and independent research.

Chapter 3. Empirical Analysis

This chapter examines the state's differentiating approaches to Russian ICT companies in the wartime and geopolitical isolation. It is based on the idea that the Russian state does not act uniformly but selectively favors or punishes firms depending on their structural characteristics and strategic behavior that reflects the degree of their loyalty.

Institutional Policies Supporting the ICT Sector

In their Routledge Handbook of Russian Politics and Society chapter, Yablokov and Solovyeva (2022) explain that in recent years the Russian government has strengthened control over ICT sector without completely nationalizing it. Rather than assuming ownership, the state facilitates close partnerships with private technology firms by providing them with exclusive privileges – such as access to state contracts or supportive regulations – based on whether they are aligned with the government's political course. Accredited IT companies may enjoy benefits such as preferential taxation, simplified visa regimes for foreign specialists, and inclusion in state procurement. Funds like the Russian Fund for the Development of Information Technologies (RFRIT), and development institutions like Skolkovo and the Internet Initiatives Development Fund (IIDF), also serve to channel financial and infrastructural support to selected firms. These support mechanisms have only intensified since 2022, as the state prioritized technological sovereignty in the face of world-scale sanctions.

Russian IT companies and startups were already highly competitive in the domestic market prior to the introduction of comprehensive sanctions. Eferin et al. (2019) argue that the competition between domestic and foreign digital platforms in Russia stimulated both innovation and growth. According to their findings, leading Russian IT companies not only succeeded in adapting to this competitive environment but often managed to occupy dominant segments of domestic market. This implies that, even before sanctions and political isolation, national firms demonstrated the ability to outperform global competitors by capitalizing on localized information, user preferences, and certain institutional advantages. This has also been expounded by Kontareva and Kenney (2022) who have shown how institutional and cultural barriers such as fragile rule of law, linguistic isolation, and political risk sheltered the domestic market from external players. Firms like Yandex and VK localized global business models to fit local needs and were hugely successful. Taken together, these works illustrate that the success of Russian IT companies in the local market was not just an effect of protectionism, but also due to their ability to innovate and localize.

In general, privileges for accredited companies can be summarized into several main measures: possibility to pay insurance contributions at reduced rates if an IT company meets the condition that the share of income from IT activities exceeds 70%; zeroing of income tax in 2022-2024 if the IT company meets the condition that the share of income from IT activities exceeds 70%; zero income tax in 2022-2024 if the IT company meets the condition that the share of income from IT activities exceeds 70%; preferential IT mortgages at a rate of up to 6% per annum for employees of IT companies; exemption from audits of state and municipal control bodies and field tax audits in 2022-2024; granting exemption from military service to employees of accredited IT companies; simplification of employment and residence permit procedures for foreign citizens who work in accredited IT companies (Ministry of Digital Development,

Communications and Mass Media of the Russian Federation, n.d.). State-owned IT clusters such as Skolkovo and Innopolis illustrate the co-optation mechanism through the creation of privileged ecosystems. Participation in these projects gives firms access to tax benefits (e.g. zero VAT for Skolkovo residents), development grants, and infrastructure support. However, such benefits often come with informal obligations – for example, a focus on “nationally significant” technologies (import substitution, cybersecurity, military technology) or the need to align strategies with government curators (Government of the Russian Federation, 2019; Skolkovo Decree No. 1172, 2010). This creates a segmented market where “loyal” companies receive competitive preferences, while independent startups remain on the periphery and do on their own regardless of the social significance of their products.

Institutional Mechanisms of Control and Constraint

However, the status of an “accredited” company can easily be backtracked. Especially considering quite specific requirements for this status. Decree No. 83, released in March 2022 by the Ministry of Digital Development, established a list of IT firms that are eligible for state support, granting privileges like military service deferment, tax advantages, and facilitation of visa entry. The register was updated in 2023, with tighter qualifications excluding firms that have changed legal residency to a foreign country, lost accreditation through partial relocation, or failed to comply with domestic software compliance requirements (Federal Law No. 83-FZ, 2022).

Yarovaya Law and the Sovereign Internet Law force providers to adhere to strict rules, such as keeping users’ data within Russia and granting access to security services. These companies

that disobedience can be penalized with fines, bans on services, or pressure on their management. In certain instances, the state may acquire partial ownership or place aligned executives in private firms, thereby bringing them firmly under government objectives. This framework, referred to as “technational corporatism,” facilitates state management of digital instruments and online platforms through the control of private firms’ activities, particularly in matters of censorship, surveillance, and internet administration. Yandex, VKontakte (VK), and Sber’s online platforms are excellent examples illustrating the fuzzy boundary between the private and public sector (Yablokov & Solovyeva, 2022), including the fact these firms possess both high organizational and high structural powers.

Russian government has heavily relied on IT specialists and companies in its pursuit of digital innovations, ranging from an e-government services portal (Gosuslugi) to advanced facial recognition systems powered by neural networks. However, the latter is considered a key element of digital authoritarianism by many researchers, as it is, for example, in China (Polyakova & Meserole, 2019). Russian government always emphasized how it makes bureaucratic chores more efficient, while human rights activists and opposition leaders pointed out how it makes Russia a surveillance state where all citizens’ personal data is collected without their consent and used against them to control, frighten, and punish. One of the brightest examples of this duality is the face recognition system in the Moscow Metro, which was praised for being innovative by pro-government speakers (it allows one to pay for entrance with face) (The Moscow Times, 2021). The facial recognition system in the Moscow Metro is being introduced and maintained by NTechLab, working in collaboration with Rostec and the Moscow government. It scans the faces of all Metro passengers and can be used by the government to effectively search for individuals: this system is responsible for arresting and

sending people to military service after 2022 (Churmanova, 2022). Russian IT sector is not only a successful economic enterprise but also a government asset that provides coercive capabilities. This became even more clear when initiatives to digitalize military service became a reality (Stanovaya, 2023). For example, official electronic summons are issued by the military commissariat and sent through the e-government platform Gosuslugi. On May 9, 2025, Russia launched the Unified Electronic Register of Subpoenas (Reestrpovestok.rf). This platform allows citizens to access military summonses online³ (Meduza, 2025).

After February 24, 2022, the Russian regime entered a period of extreme political centralization and digital militarization. The state continued to rely on digital technologies for both civil administration and repressive control, making the ICT sector strategically indispensable but also politically vulnerable. During Russian and Ukrainian conflict, military significance of the IT industry has increased significantly. This integration of military goals and civilian digital infrastructure has militarized the structural role of the IT sector as a whole. Civilian technologies like cloud platforms, geolocation services, and AI are being increasingly incorporated into defense and surveillance infrastructure even before the beginning of the war (Soldatov & Borogan, 2022). This has increased the risks of being (or perceived as) unaligned with state goals for the firms: the militarization of digital infrastructure has blurred the line between civilian and strategic technology, raising political stakes for IT firms.

³ Subpoenas considered served seven days after publication in the register, regardless of personal notification. Failure to comply within 20 days can result in restrictions such as travel bans, suspension of driving licenses, restrictions on real estate transactions, and access to credit (Meduza, 2025).

Selectivity and Room for Maneuver: Insights from Prior Research

Importantly, not all firms are treated equally. While many studies treat ICT firms in autocracies as passive recipients of state control, this research emphasizes their agency. Drawing from literature on adaptive informal institutions (Tsai, 2007), strategic authoritarianism (Gerschewski, 2013), and business-state relations in Russia (Frye, 2010; Szakonyi, 2020), this chapter emphasizes that firms keep some space for maneuver depending on their perceived strategic importance and political behavior.

Some firms have retained their privileges by cultivating political loyalty or embedding themselves in strategic infrastructure. Others, despite their previous size or economic contribution, lost access to benefits due to relocation, dissent, or misalignment with state ideology. Others have gained new structural importance by substituting sanctioned technologies.

The core empirical puzzle is: why are certain IT firms rewarded while others are excluded or even punished? This chapter addresses that question by testing hypotheses developed earlier, using case studies to assess how the interplay of firm behavior and institutional position shapes state response. In so doing, it contributes not only to our understanding of Russia's evolving digital authoritarianism, but to broader debates on firm agency, informal institutions, and state-business relations in illiberal regimes.

Dynamics of structural power

Yandex offers a robust boundary case to examine how structural power is both undermined and reconfigured in an authoritarian setting. Yandex is the largest private IT company in Russia, founded in 1997, providing a wide range of digital services: from search engine and advertising to cloud technologies, navigation, taxi services, food delivery and artificial intelligence. Until 2022, Yandex was considered the Russian equivalent of Google in terms of scale and influence on the country's digital ecosystem, although it is more comparable to Chinese WeChat. However, after the outbreak of full-scale war in Ukraine, Yandex came under pressure from both the government and the international community, leading to a restructuring and separation of the business. In July 2024, Yandex completed the sale of its Russian assets to a consortium of Russian investors for \$5.4 billion what also included one of the largest oil companies. The deal marked the end of Yandex's foreign ownership and potentially increased the Kremlin's control over the internet and technology in Russia. Following the sale, the company's international projects, including developments in artificial intelligence and autonomous driving, were retained and continued under a completely new structure led by former Yandex's CEO Arkady Volozh. Yandex N.V., the parent firm with headquarters based in the Netherlands, initiated a large-scale restructuring relocating core employees and R&D functions offshore (The Moscow Times, 2024). These mechanisms eroded the firm's embeddedness in Russian critical infrastructure and led to the gradual decline of political backing and institutional support over time. To this extent, Yandex's innovation-oriented segments exhibit the logic of Hypothesis 1a: that firms losing structural power due to relocation, brain drain, or technology decoupling⁴ put themselves at risk of marginalization in

⁴ Technology decoupling refers to the deliberate process of separating or reducing interdependence between countries or firms in the development, production, and use of technology. It often occurs due to geopolitical tensions, trade restrictions, national security concerns, or efforts to achieve technological sovereignty.

state industrial policy. However, it is noteworthy that in the case of Yandex's Russian division, holds the supposition proposed in H1a. Yandex is a borderline yet prominent case, and it could possibly be applied to any other strategically important and expensive company that may experience such a division in the future or in other countries.

On the other hand, hypothesis H1b implies that a firm which has gained structural power after 2022 receives supportive treatment from the state even if it previously lacked it. The case of Astra Group – a developer of a Russian operating system and cybersecurity solutions – exemplifies how firms can acquire structural power in a post-sanctions environment by filling critical technological gaps. Its key product Astra Linux is an operating system based on the Linux kernel, which is being implemented in Russian state organizations as an alternative to Microsoft Windows, Red Hat Enterprise Linux and Linux Ubuntu – these firms left the Russian market reacting to full-scale invasion of Ukraine. Astra Linux is certified for handling classified information up to “top secret” levels by the Ministry of Defense of the Russian Federation, FSTEC and FSB of Russia, and included in the Unified Register of Russian Programs of the Ministry of Communications of the Russian Federation since 2019 (CNews, 2020). Despite this and the fact that some government organizations adopted this OS (for example, some regional healthcare enterprises have been using this OS for their operations), prior to 2022 Astra Group could be called a niche player in Russia’s operation system market. Western alternatives like Microsoft Windows and Red Hat prevailed in the market, including regular users and state organizations. Although Vladimir Putin issued a decree ordering the transition of federal executive bodies to the use of free software in 2010, the usage of foreign software at government bodies and facilities that process critical information was ultimately forbidden only in 2022 (Awake Nerd, 2024, Federal Law No. 149-FZ, 2006). Leveraging its

compliance with strict Federal Security Service (FSB) and Federal Service for Technical and Export Control (FSTEC) certifications, Astra Linux rapidly became the de facto standard for government IT infrastructure. Regulatory mandates, such as Ministry of Digital Development Order No. 250 (2022), explicitly prioritized its adoption, propelling its market share in state institutions from under 5% to over 90% by 2024. This case underscores how firms that provide indispensable import-substitution solutions can secure state support, irrespective of their earlier market position. The state's reliance on Astra Linux for national security and bureaucratic continuity transformed it from a marginal actor into a monopolist, proving that structural power gained through technological substitution can compensate pre-existing institutional disadvantages. The material effects of this transformation are reflected in Astra Group's revenue, which expanded from 2.37 billion rubles in 2021 to 9.54 billion rubles in 2023 – it marks the growth of over 300%. Sales of the Astra Linux product line alone increased from 1.65 billion to 6.3 billion rubles over the same period (Astra Group, 2024; CNews, 2022, 2023).

This case offers strong support for H1b. The state's dependence on domestic substitutes for important foreign technologies has led to the creation of support mechanisms, and the firm happened to be in the right place at the right time, providing its product, for which it received further promotion, and its structural power has been reinforced.

Dynamics of organizational power

Moving on to the second group of hypotheses on how firms with varying degrees of organizational power can receive either a carrot or a stick from the state, it is worth recalling a very telling case. One of the clearest illustrations of how the Russian government reacts to the

loss of organizational power is the case of Group-IB, a leading cybersecurity firm that used to be engaged in state cybercrime prevention efforts. Founded by Ilya Sachkov, the company was in near constant contact with security and law enforcement agencies, holding joint operations with the Ministry of Internal Affairs and reportedly with the FSB. However, this relationship took a dramatic turn with the arrest of Sachkov in September 2021 on charges of espionage and treason, having allegedly transferred classified information to foreign intelligence services (Reuters, 2024). Although the arrest occurred before the full-scale invasion of Ukraine, the problems for the company escalated within the post-2022 scenario. After relocating its global headquarters to Singapore and delinking its operations from Russian state interests, Group-IB lost reputationally and faced a de facto prohibition on public procurement and high-prestige contracts (Cyprus Mail, 2024). Media coverage of the company turned negative, framing internationalization as a betrayal of national interests. The state no longer viewed Group-IB as part of the country's sovereign digital infrastructure.

In 2024, Russia's Ministry of Digital Development (MinTsifry) rescinded over 2000 IT firms' accreditation as part of a broad campaign to, presumably, revise eligibility criteria and reduce government expenditure on IT support measures. In October of 2022, the government introduced new accreditation requirements in the form of at least 30% IT-reliant revenue, a primary IT business activity (by OKVED – All-Russian Classifier of Economic Activities), and workers' salaries at or close to regional levels. The reform also excluded institutions with over 50% state ownership, telecommunications operators, banks, and state institutions (CNews, 2022). Some of the delisted organizations include well-known entities such as Rostec and Rostelecom affiliates, the Digital Economy League, and notably, the High Technology

Technopark “IT-Park” of Tatarstan – the country's first government-initiated technopark (CNews, 2024; Zoom CNews, 2024).

A developed and advanced IT sector was the objective success of post-Soviet Russia. The sphere originates deep in the USSR's technical and mathematical schools of sciences which were accessible to people from different backgrounds and were free from the influence of ideology unlike sociology or historical science with its rigid Marxist inclination. IT infrastructure began to develop actively under the presidency of Dmitry Medvedev (2008-2012), who was known for his support of innovation and technology. At the same time, the Skolkovo IT cluster in Odintsovo of the Moscow region was established. There is even technology parks engaged in defense technologies (e.g., Almaz-Antey Concern). Officially Technopark in the Sphere of High Technologies “IT Park”) is a state-backed technology hub in Tatarstan, established to become a key instrument in regional digitalization policy, support sanctions-proof innovation, and integrate regional firms into federal import-substitution programs Founded in 2012 under Tatarstan’s Ministry of Digital Development, with federal backing from MinTsifry and Rostec, it receives subsidies from the National Technology Initiative (NTI) and Skolkovo Foundation for priority projects what indicates a high degree of organizational power. The park was designed not just to house IT startups but to have big companies and public – private R&D partnerships too. Throughout its operational years, the park welcomed over 150 firms: among them were top national and global brands like ICL Services, FIX, Acronis, and ABBYY. The Technopark played the main role of incorporating Tatar IT companies into federal-level initiatives (Tatar-inform, 2015).

With the beginning of war, many companies left Technopark, thereby reducing its structural power. Among these companies was ABBYY, which relocated to Armenia. However, from an organizational power perspective, things were looking up: the IT park in Kazan significantly expanded its infrastructure, strengthened its support for startups and educational initiatives, and achieved significant economic success – all with the active support of the Tatarstan government. In July 2024, IT Park was unexpectedly removed from the federal list of accredited IT companies. This occurred despite its long-standing institutional ties and symbolic status in Russia's digital modernization policy. Removal from the register automatically deprived the company of benefits such as tax breaks, subsidies, and, what is particularly important in wartime, deferment of employee conscription into the army. The ministry did not officially justify its decision in detail, but observers noted that the revised accreditation standards placed greater emphasis not only on financial thresholds but also on increasingly strict formal compliance with federal policy guidelines – requirements that even government programs may not meet in the context of changing priorities (Zoom CNews, 2024).

This example convincingly refutes the hypothesis H2b: organizational power, historically strong and built on federal programs, can even strengthen under new wartime circumstances, however, it does not always serve as a shield from state's "sticks" implemented in the form of withdrawal of previously given incentives.

Political loyalty of Russian IT-firms

The case of Tinkoff Bank, later renamed to T-Bank and now operating under this name, can serve as a textbook example for the hypothesis that a firm can face punishment despite having

high powers if it does not display political loyalty. Its clientele exceeds 40 million users, making it one of the biggest online banks in Russia after state-aligned titans such as Sberbank and VTB (Tinkoff Group, n.d.). The bank underwent a forced change in ownership and title following the publicized anti-war opinions of its founder Oleg Tinkov, a widely known Russian businessman. The rebranding was seen by the experts as an attempt to erase all traces of its dissident founder, who responded mockingly to the move: “T-Bank? They might as well have called it Z-Bank” – a scathing attack on the militaristic symbolism embraced by the Kremlin wartime propaganda (Meduza, 2024).

Founded by Oleg Tinkov in 2006, Tinkoff Bank had grown into one of Russia’s most prominent fintech institutions by 2022, operating a sophisticated digital ecosystem including banking, insurance, and investment services. The headquarters were manned by around 70% IT professionals, further cementing the business as a tech company (The Banker, 2021).

Despite the firm’s size and its noticeable presence in the digital economy, the bank's founder made headlines in April 2022 when he publicly condemned Russia's actions in Ukraine as a “massacre” and criticized Russian military (El País, 2022). This political disobedience led to prompt backlash. According to Tinkov, the Kremlin pressured the bank's management to sever ties with him, threatening with nationalization of the assets if they refused. The businessman was forced to sell his 35% stake in TCS Group at a significantly cut-price to Vladimir Potanin's Interros Group (The Moscow Times, 2022). Notably, Vladimir Potanin is also a beneficiary of Yandex’s share sells. This person is the president of Norilsk Nickel, second in Forbes' ranking of Russia's richest billionaires, and former member of Yeltsin's administration. However, even more interesting acquisitions and alliances are taking place in modern Russia. The story of

Wildberries, an online marketplace and IT company, was marked by a shootout in Moscow and support for the conflicting parties from Ramzan Kadyrov and Senator Suleiman Kerimov. But this goes beyond the scope of the current research.

Discussion of the results

This section summarizes the empirical patterns uncovered in the analysis and evaluates the four hypotheses in light of the cases I studied. It also reflects the broader theoretical implications for understanding selective governance and firm-state relations in authoritarian settings, particularly in the context of ongoing war.

Yandex, once the most structurally embedded IT firm in the country, was forced to restructure and divest its Russian assets. The case suggests that structural power offers only partial protection in wartime Russia, and at the same time this confirms H1a: structural power can erode due to relocation, technological decoupling, or ownership restructuring – each of which weakens a firm’s embeddedness in state-critical infrastructure and increases its exposure to marginalization.

Tinkoff’s trajectory demonstrates the vulnerability of structural power in an autocratic environment – as indicated in Table 1, such takeover explicitly represents the state’s “sticks”. This rebranding symbolically represented the triumph of political restraint over entrepreneurial liberty, showing that innovation loses in the face of political conjuncture. In spite of its enormous customer base and technological influence, the firm’s link to an unreliable member

of the elite proved sufficient reason for a state-led shift in ownership and obliteration of reputation. This confirms that in post-2022 Russia, political loyalty is now a condition for continued access to state favor and legal protection – irrespective of a firm's past contributions to strategic sectors or innovation value.

On the other hand, Astra Linux's case strongly supports H1b and shows that firms can gain structural power by becoming indispensable to the regime's agenda of technological sovereignty and import substitution. Astra Linux became a core supplier for secure state digital infrastructure, receiving regulatory prioritization and substantial revenue growth. This illustrates the state's instrumental logic. By offering selective subsidies, state contracts, or regulatory exemptions to favored firms (e.g., those developing "critical" technologies like import-substituted software or surveillance tools or military technologies), the regime creates a tiered market with its "insider" firms. They benefit from public procurement ("goszakupki") (e.g., the "Digital Economy" program) which prioritizes funding for domestic IT solutions in sectors like cybersecurity and big data (Government of the Russian Federation, 2017).

"A firm losing organizational power – whether through leadership targeting, relocation, or deviation from state agendas – faces the revocation of incentives", says H2a, and the case of Group-IB strongly supports this. Firms are penalized not just for political disagreement but also for exiting the institutional space of state-driven technological sovereignty. Tatarstan IT Park case shows that companies based on local or semi-autonomous innovation systems can be particularly vulnerable when central authorities take control of IT support funds and restore loyalty and usefulness according to stricter standards.

However, this assumption requires further testing. The case has possible implications for the studies of Russian asymmetric federalism – where regional ties become liabilities under centralization.

In both cases, strong historical embeddedness within state-led programs or law enforcement partnerships did not prevent eventual exclusion from state support mechanisms. Group-IB, – a case reviewed in relation to H2b – once a key actor in state cybersecurity policy, was abandoned following the criminal prosecution of its founder and the firm's relocation abroad. IT-Park in Tatarstan, despite being a government-established technopark and host to dozens of federal-level initiatives, lost its accreditation in 2024 – suggesting that symbolic institutional capital alone does not guarantee future privileges. A firm losing organizational power – whether through leadership targeting, relocation, or deviation from state agendas – faces the revocation of incentives.

One could even say that the state actions are cynical, however, it aligns with the logic of crony (state) capitalism (Haber; Kang, 2002; Aslund, 2019). However, as Tinkoff case confirms, even highly digital firms can be punished if they (or their founders) show disloyalty. These cases suggest a need to revise the initial assumption of my hypotheses: organizational and/or structural power, while enabling access to state support, does not ensure protection unless it is constantly reaffirmed through behavior, formal compliance, and perceived loyalty. This reflects the broader mechanism of “coercive loyalty” described by Guriev and Treisman

(2022), where authoritarian regimes do not simply reward insiders, but continuously test and discipline them.

This dynamic aligns with theories of strategic authoritarianism (Gerschewski, 2013), where coercive, co-optative, and legitimating strategies are deployed flexibly: based on regime needs. In this sense, the organizational power of IT firms in Russia under wartime conditions appears conditional, revocable, and more reputational than legal. Its utility for the state must be persistent and performative, like it is for the firms that obtain structural power.

Conclusion

This study shows that the Russian state's approach to managing the ICT sector after its full-scale invasion of Ukraine in 2022 is neither uniformly benevolent nor purely repressive. Instead, it can be imagined as a system of selective patronage, in which structural and organizational power – along with presumed political loyalty – determines a firm's access to “carrots” or exposure to “sticks”. Russia's IT sector is being reshaped into a hierarchical patronage system, where “carrots” include subsidies for import substitution and military draft deterrents, while non-compliant firms get some form of punishment - “sticks”, conceptualized in this research as a wide variety of measures (see Table 1).

The emigration of qualified IT specialists, followed by the outbreak of full-scale invasion, outflow of their earned income and reduce in tax base posed a significant problem for the Russian state and especially for Russian IT giants. These specialists formed a critical part of Russia's digital infrastructure and innovation economy which had been built in span of the whole history of young Russian state. This is yet another wave of emigration that the Russian people have faced throughout the country's history. Based on my analysis, it can be assumed that short-term revenue gains (e.g., Astra's growth) mask long-term R&D stagnation due to brain drain. And as always, it will not go unnoticed and will have long-lasting consequences starting from staff shortage and ending with another demographic crisis enforced by military losses.

With the full-scale invasion to Ukraine, Russia has been subject to sanctions in many industries. The United States, European Union, and other allied nations have implemented a broad array of sanction policies targeting various sectors, including finance, energy, and key individuals within Russian political landscape. The effect of the war and induced sanctions, however, is believed to be less pronounced than it was expected by the expert community (Yushkov & Alexeev 2024). There is an ongoing discussion why sanctions may not work. Starting from 2014 when Russia annexed Crimea Peninsula and backed insurgency in Donetsk and Luhansk regions, territories of Ukraine. Although the sanctions create significant financial pressure on Russian companies, they have not led to a significant long-term deterioration in the economic performance of sanctioned firms. In the short term, there is a decrease in indicators (turnover, employment), but over time this impact weakens (Gaur, Settles & Väättänen 2023). With the full-scale invasion of Russia, this problem has become more important and critically practice-oriented. While the war is continuing, any study of sanction policy effectiveness may be considered as the base for further decisions and policy developments. And, it is believed, an analysis of the economic situation of private and public actors in Russia may be useful.

Of course, it should be noted that this research has its own serious *limitations*: internal corporate data or unpublished decisions on accreditation/delisting is unavailable for outsiders, thus it is only possible to conduct mostly qualitative, case-based study without statistical modeling on large-N dataset. Prospect for additional studies on the subject is formalization of indicators and variables to secure more robust results or small-n process-tracing. Another possible suggestion could be a series of expert interviews, if not with the firms' management, then with players actively involved in the field. The other thing is that discussion of sanctions is limited under the current framework, while western sanctions have reshaped state-firm relations (e.g., import

substitution policies). This could also be explored further, attracting international players as the third party in the analysis.

It gives us an idea of what might happen in other illiberal regimes, such as China. Some regimes where cronyism can be observed, are more dependent on the capital of major market players and business elites. It can be said that crony capitalism's binary logic (loyalty vs. exclusion) oversimplifies firm agency and many Russian IT companies engage in "strategic hedging" balancing state demands with global market integration. This leads us to another limitation of the study: as the state strikes a balance between incentive and repressive policies, employing one or the other, many firms too are balancing to remain, if anything, part of the global economic system. External forces are the third party, which we unfortunately cannot exclude at the moment, but it is a good point to look for further research. Some firms like Wargaming obtain significant structural power but originate in Belarus. It is another possible venue for future studies – to explore companies that originate from both of so-called "Union State" or even CIS countries which host many of the companies that have left Russia, including Kazakhstan, Armenia and others.

The war has turned Russia's digital economy into a testing ground for twenty-first-century authoritarian governance. Selective repression and incentive distribution are used not just to silence dissent, but to re-engineer market hierarchies. In this context, the ability of IT firms to remain adaptive, loyal, or useful to the state defines their survival.

Bibliography

Abramova, A., & Garanina, O. (2018). Russian MNEs under sanctions: Challenges for upgrading in GVCs (Cases of energy and IT industries). **Journal of East-West Business*, 24*(4), 371–391. <https://doi.org/10.1080/10669868.2018.1515859>

AK&M. (2023, August 23). 3.46 million shares of Baikal Electronics will go under the hammer. <https://www.akm.ru/eng/news/3-46-million-shares-of-baikal-electronics-will-go-under-the-hammer/>

Analytical Center under the Government of the Russian Federation. (2024, November 7). Moscow IT companies increased their turnover in the first nine months of 2024. <https://en.ac-mos.ru/news/1956/>

Astra Group. (2024, April 2). Выручка «Группы Астра» за 2023 год выросла на 77% и обновила исторический максимум [Astra Group's revenue for 2023 grew by 77% and reached a new all-time high]. <https://astra.ru/about/press-center/news/vyruchka-gruppy-astra-za-2023-god-vyroslo-na-77-i-obnovila-istoricheskiy-maksimum-/>

Baikal Electronics. (2021). О компании [About the company]. <https://www.baikalelectronics.ru/company/>

Business-Gazeta. (2021, December 9). Ruslan Vlasov: “IT Park’s revenue has exceeded 17 billion rubles” [in Russian]. <https://www.business-gazeta.ru/article/539135>

The Banker. (2021). Russia’s Tinkoff builds out its AI strategy. <https://www.thebanker.com/Digital-journeys/Russia-s-Tinkoff-builds-out-its-AI-strategy>

The Bell. (2022, November 21). Russia's IT exodus and the Kremlin's futile efforts to reverse it. <https://en.thebell.io/russia-s-it-exodus-and-the-kremlin-s-futile-efforts-to-reverse-it/>

Churmanova, K. (2022, October 24). Из метро – на фронт. Как власти Москвы следят за “уклонистами” с помощью системы распознавания лиц [From the subway to the front. How Moscow authorities track “evaders” using facial recognition]. BBC Russian. <https://www.bbc.com/russian/features-63346138>

CNews. (2020, April 13). Отечественную ОС Astra Linux установили на более чем 52 000 рабочих мест в госструктурах [Domestic OS Astra Linux installed on more than 52 000 workstations in government agencies]. https://www.cnews.ru/news/top/2020-04-13_otechestvennuyu_os_astra_linux_ustanovili

CNews. (2022, May 11). Прибыль разработчика главной российской ОС перевалила за миллиард [Profit of the main Russian OS developer exceeded 1 billion]. https://www.cnews.ru/news/top/2022-05-11_pribyl_razrabotchika_glavnoj

CNews. (2022, November 25). Минцифры “зачищает” реестр аккредитованных ИТ-компаний [Ministry of Digital Development “cleans up” the register of accredited IT companies]. https://itsupport.cnews.ru/news/top/2022-11-25_mintsifry_zachishchaet_reestr

CNews. (2023, November 21). Создатели Astra Linux заявили о двукратном росте выручки [Astra Linux reports doubling of revenue]. https://www.cnews.ru/news/top/2023-11-21_razrabotchik_astra_linux_otchitalsya

CNews. (2024, July 22). Две тысячи российских ИТ-компаний лишились аккредитации [Two thousand Russian IT companies lose accreditation]. https://www.cnews.ru/news/top/2024-07-22_dve_tysyachi_rossijskih_kompanij

Cyprus Mail. (2024, February 10). After months of negotiation, a rare Russian compromise as Yandex changes hands. <https://cyprus-mail.com/2024/02/10/after-months-of-negotiation-a-rare-russian-compromise-as-yandex-changes-hands/>

Djankov, S. (2015). Russia's economy under Putin: From crony capitalism to state capitalism (Policy Brief No. PB15-18). Peterson Institute for International Economics. <https://www.piie.com/publications/policy-briefs/russias-economy-under-putin-crony-capitalism-state-capitalism>

Eferin, Y., Hohlov, Y., & Rossotto, C. (2019). Digital platforms in Russia: Competition between national and foreign multi-sided platforms stimulates growth and innovation. *Digital Policy, Regulation and Governance*, 21(2), 129–145. <https://doi.org/10.1108/DPRG-08-2018-0046>

El País. (2022, May 5). Tinkov, the Russian oligarch who lost his bank for criticizing Putin's invasion. <https://english.elpais.com/international/2022-05-05/tinkov-the-russian-oligarch-who-lost-his-bank-for-criticizing-putins-invasion.html>

Federal Law No. 149-FZ of July 27, 2006. (2006). On information, information technologies and information protection [Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»]. Consultant.ru. https://www.consultant.ru/document/cons_doc_LAW_111346/

Federal Law No. 34-FZ of March 2, 2022. (2022). On amendments to the Federal Law "On information, information technologies and information protection" [Федеральный закон от 02.03.2022 № 34-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»»]. Official Internet Portal of Legal Information. <http://publication.pravo.gov.ru/Document/View/0001202203020001>

Federal State Statistics Service. (2023). Information Society in the Russian Federation: 2023 (Statistical Collection). <https://rosstat.gov.ru/folder/210/document/13223>

Forbes. (2025, February 21). Иногда они возвращаются: как российские ИТ-компании заняли место иностранных [Sometimes they return: How Russian IT companies took the place of foreign ones]. <https://www.forbes.ru/mneniya/531097-inogda-oni-vozvrasautsa-kak-rossijskie-it-kompanii-zanali-mesto-inostrannyh>

Freedom House. (2021). Freedom on the Net 2021: Belarus. <https://freedomhouse.org/country/belarus/freedom-net/2021>

Frye, T. (2010). Building states and markets after communism: The perils of polarized democracy. Cambridge University Press.

Gaur, A., Settles, A., & Väättänen, J. (2023). Do economic sanctions work? Evidence from the Russia-Ukraine conflict. *Journal of Management Studies*, 60(6), 1391–1414. <https://doi.org/10.1111/joms.12931>

Gerschewski, J. (2013). The three pillars of stability: Legitimation, repression, and co-optation in autocratic regimes. *Democratization*, 20(1), 13–38. <https://doi.org/10.1080/13510347.2013.738860>

Government of the Russian Federation. (2017). On the approval of the program “Digital Economy of the Russian Federation” [Об утверждении программы «Цифровая экономика Российской Федерации», Постановление Правительства РФ от 28 июля 2017 г. № 1632-п]. <https://publication.pravo.gov.ru/Document/View/0001201708040001>

Government of the Russian Federation. (2019). On measures of state support in the field of the digital economy [О мерах государственной поддержки в сфере цифровой экономики, Постановление Правительства РФ от 4 декабря 2019 г. № 1609]. <https://publication.pravo.gov.ru/Document/View/0001201912050007>

Government of the Russian Federation. (2022, March 6). Decree No. 299 on amendments to the methodology for determining the amount of compensation paid to a patent holder when deciding to use an invention without their consent. <https://www.garant.ru/products/ipo/prime/doc/404259510/>

Government Services. (n.d.). IT industry [IT-отрасль]. Gosuslugi. Retrieved April 15, 2025, from <https://www.gosuslugi.ru/itindustry>

Gritsenko, D., & Indukaev, A. (2021). Digitalising city governance in Russia: The case of the ‘active citizen’ platform. **Europe-Asia Studies*, 73*(6), 1102–1124. <https://doi.org/10.1080/09668136.2021.1945485>

Guriev, S., & Treisman, D. (2015). How modern dictators survive: Cooptation, censorship, propaganda, and repression. *Annual Review of Political Science*, 19, 565–587. <https://doi.org/10.1146/annurev-polisci-062813-051249>

Haber, S. (2002). *Crony capitalism and economic growth in Latin America: Theory and evidence*. Hoover Institution Press.

Szakonyi, D. (2020). *Politics for profit: Business, elections, and policymaking in Russia*. Cambridge University Press.

Hellman, J. S. (1998). Winners take all: The politics of partial reform in postcommunist transitions. *World Politics*, 50(2), 203–234. <https://doi.org/10.1017/S0043887100008091>

Kamalov, E., Kostenko, V., Sergeeva, I., & Zavadskaya, M. (2022, September 6). *Russia’s 2022 anti-war exodus: The attitudes and expectations of Russian migrants* (Policy Memo No. 790). PONARS Eurasia. <https://www.ponarseurasia.org/russias-2022-anti-war-exodus-the-attitudes-and-expectations-of-russian-migrants/>

Kamalov, E., Nugumanova, K., & Sergeeva, I. (2025). On the Move: Mobility, Integration, and the Dynamics of Russian Emigration in 2022–2024. OutRush. https://outrush.io/report_march_2025_eng

Kang, D. C. (2002). *Crony capitalism: Corruption and development in South Korea and the Philippines*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511606175>

Kontareva, A., & Kenney, M. (2023). National markets in a world of global platform giants: The persistence of Russian domestic competitors. *Policy & Internet*, 15(3), 327–350. <https://doi.org/10.1002/poi3.344>

Kravits-Meinke, D. (2024, May 15). The sad fate of Yandex: From independent tech startup to Kremlin propaganda tool. Centre for East European and International Studies (ZOiS). <https://www.zois-berlin.de/en/publications/zois-spotlight/the-sad-fate-of-yandex-from-independent-tech-startup-to-kremlin-propaganda-tool>

Kuleshova, G. I. (2020, February). Scientific bases of spatial development of innovative activity in the territory of Russia. In *IOP Conference Series: Materials Science and Engineering* (Vol. 753, No. 5, p. 052070). IOP Publishing.

Laporte, J. (2022). Russia's superpresidency. *Russian Politics Today: Stability and Fragility*, 33, 45–62.

Levitsky, S., & Way, L. A. (2010). *Competitive authoritarianism: Hybrid regimes after the Cold War*. Cambridge University Press.

Litvinov, D. (2024, March 30). IT Entrepreneurs in 2024: How the most technological segment of small and medium business will develop. *RB.ru*. <https://rb.ru/opinion/itpredprinimateli2024/>

Mann, M. (1984). The autonomous power of the state: Its origins, mechanisms and results. *European Journal of Sociology*, 25(2), 185–213. <https://doi.org/10.1017/S0003975600004239>

Matveev, I. (2019). Big business in Putin's Russia: Structural and instrumental power. **Demokratizatsiya: The Journal of Post-Soviet Democratization*, 27*(4), 401–422.

Meduza. (2023, May 10). Yandex goes Dutch: In an effort to divest itself of its Russian segment, the multinational IT giant is looking to create a ‘consortium’ of oligarch shareholders, while distancing from the Kremlin. <https://meduza.io/en/feature/2023/05/10/yandex-goes-dutch>

Meduza. (2024, March 27). Half the processors made by Russian chipmaker Baikal Electronics are reportedly defective. <https://meduza.io/en/news/2024/03/27/half-the-processors-made-by-russian-computer-chipmaker-baikal-electronics-are-reportedly-defective>

Meduza. (2025, May 9). В России заработал реестр электронных повесток [Russia launches electronic draft notices registry]. <https://meduza.io/news/2025/05/09/v-rossii-zarabotal-reestr-elektronnyh-povestok>

Ministry of Digital Development, Communications and Mass Media of the Russian Federation. (n.d.). State services in digital form. *Digital.Gov.Ru*. Retrieved April 3, 2025, from <https://digital.gov.ru/ru/activity/govservices/1/>

Ministry of Digital Development, Communications and Mass Media of the Russian Federation. (n.d.). List of systemically important organisations in the information and communication technology sector. Retrieved May 26, 2025, from <https://digital.gov.ru/uploaded/files/perechen-sistemoobrazuyuschih-organizatsij.xls>

The Moscow Times. (2021, October 15). Moscow Metro introduces ‘world’s first’ pay-by-face system. <https://www.themoscowtimes.com/2021/10/15/moscow-metro-introduces-worlds-first-pay-by-face-system-a75300>

The Moscow Times. (2022, May 2). Russian bank founder says Kremlin forced sale of his group stake. <https://www.themoscowtimes.com/2022/05/02/russian-bank-founder-says-kremlin-forced-sale-of-his-group-stake-a77555>

The Moscow Times. (2024, July 15). Yandex parent company fully divests from Russia. <https://www.themoscowtimes.com/2024/07/15/yandex-parent-company-fully-divests-from-russia-a85714>

Polyakova, A., & Meserole, C. (2019). Exporting digital authoritarianism: The Russian and Chinese models (Policy Brief No. PB19-29). Brookings Institution.

President of the Russian Federation. (2022, March 2). Decree No. 83: On measures to ensure the accelerated development of the information technology industry in the Russian Federation. <http://publication.pravo.gov.ru/Document/View/0001202203020001>

President of the Russian Federation. (2022, March 2). *Federal Law No. 30-FZ of March 2, 2022, on amendments to certain legislative acts of the Russian Federation*. <http://publication.pravo.gov.ru/Document/View/0001202203020001?index=2>

Reuters. (2024, July 27). Russia charges Group-IB founder Ilya Sachkov with treason. <https://www.reuters.com/technology/russia-charges-group-ib-founder-ilya-sachkov-treason-2024-07-27/>

Russia uses custom Linux. (2024, November 30). Awake Nerd. Retrieved May 27, 2025, from <https://awakenerd.com/2024/11/30/russia-uses-a-custom-linux/>

Shleifer, A., & Vishny, R. W. (1993). Corruption. *The Quarterly Journal of Economics*, 108(3), 599–617. <https://doi.org/10.2307/2118402>

Soldatov, A., & Borogan, I. (2022). *The Compatriots: The Brutal and Chaotic History of Russia's Exiles, Émigrés, and Agents Abroad*. PublicAffairs.

Sonin, K. (2022, September 5). Russia’s crony capitalism disincentivises economic reform. *The Economist*. <https://www.economist.com/by-invitation/2022/09/05/russias-crony-capitalism-disincentivises-economic-reform-says-konstantin-sonin>

Stanovaya, T. (2023, April 17). Russia’s new conscription law brings the digital gulag much, much closer. *Carnegie Politika*. <https://carnegieendowment.org/russia-eurasia/politika/2023/04/russias-new-conscription-law-brings-the-digital-gulag-much-much-closer>

Strange, S. (2015). *States and markets* (R. Palan, Ed.). Bloomsbury Academic.

Tatar-inform. (2015, October 23). ИТ-парку исполнилось шесть лет [IT Park turns six]. <https://www.tatar-inform.ru/news/it-parku-ispolnilos-shest-let-477174>

Tinkoff Group. (n.d.). Company summary. <https://tinkoff-group.com/company-info/summary/>

Tom's Hardware. (2023, October 20). Russian chipmaker Baikal goes bankrupt, assets valued at only \$5 million. <https://www.tomshardware.com/news/russian-chipmaker-baikal-goes-bankrupt-assets-valued-at-only-dollar5-million>

Tsai, K. S. (2006). Adaptive informal institutions and endogenous institutional change in China. *World Politics*, 59(1), 116–141. <https://doi.org/10.1353/wp.2007.0018>

Wedel, J. R. (2003). Clans, cliques and captured states: Rethinking 'transition' in Central and Eastern Europe and the former Soviet Union. *Journal of International Development*, 15(4), 427–440. <https://doi.org/10.1002/jid.993>

Yablokov, I., & Solovieva, A. (2022). The Kremlin's digital toolkit: Internet control and the logic of technocratic authoritarianism. In G. Gill & P. Hanson (Eds.), *Routledge handbook of Russian politics and society* (2nd ed., pp. 337–351). Routledge.

Yablokov, I., & Solovyeva, O. (2022). ICT in Putin's Russia: 1999–2021. In *Routledge handbook of Russian politics and society* (pp. 364–376). Routledge.

Yushkov, A., & Alexeev, M. (2024). Russian regions in wartime: Fiscal and economic effects of the Russo-Ukrainian war. **Post-Soviet Affairs*, 40*(1), 1–13. <https://doi.org/10.1080/1060586X.2024.2312345>

Zoom CNews. (2024, July 23). Из реестра аккредитованных ИТ-компаний исключили «ИТ-парк» Татарстана [IT Park Tatarstan removed from the register of accredited IT companies]. <https://zoom.cnews.ru/news/item/607814>