

Russia's large fintechs and digital ecosystems – in the face of war and sanctions

Katharina Allinger, Stephan Barisitz, Andreas Timel¹

Russia's financial landscape has changed rapidly in recent years, with the lines between banks and tech firms ever more blurring and giving rise to large fintech firms. We are going to look at these changes from a perspective before and after Russia's invasion of Ukraine in February 2022. Pre-war, tech firms such as Yandex or VK and financial firms such as Sberbank started diversifying into each other's business by broadening service offers to consumers via so-called digital ecosystems. From an international perspective, two things stand out: first, with Sberbank, Russia's largest bank is attempting to fully rebrand itself as a technology company. Second, the Russian government facilitates these developments both directly and indirectly, e.g. by pushing the country's digital transformation while simultaneously exercising more control over foreign tech firms. From a post-invasion perspective, international sanctions pose several challenges to large fintech firms; and so do economic and geopolitical developments. Going forward, the firms will face major issues in advancing their digital ecosystems. As to technology-related sanctions, we show that Russia continues to substantially depend on technologies from abroad, despite pre-war efforts to reduce this dependence. Russia's economy in general and its tech and fintech firms in particular are thus vulnerable to international technology sanctions. As to sanctions evasion, particularly through crypto assets, we currently see limited potential for circumvention. Clearly, sanctioning countries need to perceive sanctions as a dynamic tool that they must adjust regularly to address potential loopholes and circumvention tactics.

JEL classification: G20, G28, O30, F51

Keywords: fintech, digital ecosystems, Russia, sanctions

Fintech²-driven innovations and changes in the financial system have attracted much attention among policymakers and researchers. As many fintech studies focus on countries like the USA and China, it is not widely known that the Russian financial market has, in recent years, likewise seen a fast pace of financial inclusion, digitalization and adoption of fintech services (CBR, 2021c; Melkadze, 2021). Noteworthy fintech developments in Russia include (1) the growing scene of smaller fintechs, (2) the blurring lines between large financial institutions and tech firms, (3) the relatively sizeable crypto economy and (4) a digital ruble pilot recently launched by the Central Bank of the Russian Federation (CBR). The relatively advanced stage of fintech adoption in Russia may be explained by numerous factors. Among other things, banks have embarked on a digitalization drive and tech firms have started to enter finance. Russia has a strong base of science and tech graduates, and the CBR and the Russian government have taken an overall supportive stance on digitalization (see Ernst & Young, 2019; Switzerland Global Enterprise, 2021).

¹ Oesterreichische Nationalbank, Central, Eastern and Southeastern Europe Section, katharina.allinger@oenb.at and stephan.barisitz@oenb.at; Supervision Policy, Regulation and Strategy Division, andreas.timel@oenb.at. Opinions expressed by the authors of studies do not necessarily reflect the official viewpoint of the OeNB. The authors would like to thank Elisabeth Beckmann and Konrad Richter (both OeNB) and two anonymous referees for helpful comments and valuable suggestions.

² We define "fintech" broadly and in line with the European Commission as "technology-enabled innovation in financial services that could result in new business models, applications, processes or products" (see e.g. "FinTech Action plan" [EUR-Lex - 52018DC0109 - EN - EUR-Lex \(europa.eu\)](#)).

However, Russia's invasion of Ukraine on February 24, 2022, with its far-reaching political, economic and humanitarian consequences around the globe and in particular in Ukraine and Russia, is set to leave its mark on Russia's fintech developments. We try to balance the pre- and post-invasion view³ regarding one particular fintech development, namely the rise of fintech conglomerates in Russia and their digital ecosystems. Digital ecosystems include many different services (and potentially platforms⁴) which people may access via one single process, often with an app as customer interface (for an illustrative example, see figure 1) (World Bank, 2018). The financial system in Russia has been moving toward competing digital ecosystems. Such ecosystems are being built either by tech firms adding financial services to their offer (e.g. Yandex NV) or by banks diversifying their nonfinancial service portfolio (e.g. Sberbank of Russia PJSC). While the rise of digital ecosystems is not unique to Russia (see e.g. China's WeChat/Tencent or Alibaba), few countries have seen such fast progress over recent years as Russia. The aggressiveness with which Russian banks have embarked on this transformation is, however, rather unique. Particularly Sberbank, Russia's largest bank, stands out, as it aims to become a consumer technology company.

Throughout this study, when we discuss "large fintechs," we refer to businesses building digital ecosystems that include financial services. This way, we set them apart from the broader space of mostly smaller fintechs. We focus on them for two reasons. First, from a research perspective, it is exciting to examine the fast-changing financial landscape and aggressive tech expansion of Russia's largest banks as well as the regulatory challenges that this transformation entails. Second, these firms play a major role in Russia's economy given their significant size. In addition, they are now affected by difficulties at both a financial and a technological level, e.g. through sanctions and other, partly related, disruptions.

The study is structured as follows: in section 1, we provide a brief overview of digitalization in Russia and its impact on fintech developments. The latter have been strongly influenced by the Russian government's aim to transform Russia into a global digital leader, with a view to achieving digital sovereignty and reducing technological dependence on foreign countries, particularly the USA. In section 2, we discuss Russia's digital ecosystems and regulatory risks identified internationally and by the CBR. In section 3, we look at the digital ecosystems and their providers in the light of international sanctions and challenges. Given their relevance for both fintech players and the Russian economy in general, we zero in on technology-related sanctions. We also briefly discuss the potential for sanctions evasion. Section 4 concludes.

1 Murky outlook for Russia's ambition to become a global digital leader

Russia's government is keen to become a major digital player on a global scale. We analyze some of the motives behind this ambition, focusing on the government's drive to reach digital sovereignty.

³ Throughout the study, "war" refers to the military conflict that resulted from Russia's invasion of Ukraine on February 24, 2022. The cutoff date for this study was end of April 2022, but we integrated selected important developments until mid-June 2022 during the revision process. Given the fast-changing environment and complexity of the topic, we would like to note that this study has been done on a best-effort basis.

⁴ Digital platforms are information systems catalyzing multisided marketplaces. Value is created as producers and users interact (World Bank, 2018) – a famous nonfinancial example is Booking.com.

1.1 Still much to catch up on top innovators

Russia's overarching goal of becoming a global digital leader also encompasses innovations in finance. According to a report published by the World Bank (2018), digital transformation had become a top priority for Russia's government, with Russia having successfully created both digital and nondigital factors to support its digital transition – even though work remained to be done in certain areas.

The projects and initiatives launched by the Russian government include “The National Digital Economy Programme of the Russian Federation” and the “National Strategy for the Development of Artificial Intelligence for the period until 2030” (for further examples, see European Commission, 2021). On the upside, Russia has made great strides in some areas, e.g. in providing both e-government and payment systems, reportedly outstripping some Western countries (The Economist, 2022b). On the downside, the Russian government has to date failed to make substantial progress on several initiatives and targets. Cases in point are the aim to increase the share of high-tech exports or gross domestic expenditures on research and development (Epifanova and Dietrich, 2022).

Table 1 summarizes some composite indicators related to fintech, innovation and the business environment in Russia. Based on this evidence, Russia is performing quite well relative to its peer countries, here defined as the BRICS countries Brazil, India, China and South Africa. Russia tops, or at least matches, the performance of Brazil, India and South Africa⁵ on most indicators, but fares mostly worse than China. However, Russia's overall rank suggests that there is still substantial

Table 1

Russia's rank in fintech and innovation-related indices relative to BRICS countries

	Russia	Brazil	India	China	South Africa	Number of countries/cities	Russia's rank 3 years previously ¹
Country indices							
	Rank ²						
Ease of Doing Business (World Bank), 2020	29	124	62	32	84	190	40/190
Global Competitiveness Index 4.0 (World Economic Forum), 2019	43	71	68	28	60	141	43/138
Global Innovation Index (GII) (World Intellectual Property Organization), 2021	45	57	46	12	61	132	46/129
Fintech adoption rate (Ernst & Young, 2019), 2019 ³	3	16	1	1	3	27	n.a.
The Global Fintech Index (Findexable), 2021	19	14	23	15	44	83	32/65
City indices⁴							
The Global Fintech Index (Findexable), 2021	18	4	13	9	97	264	30/238
IFZ Fintech Study (IFZ, 2021), 2021	31	34	33	9	32	35	26/30

Source: Authors' compilation.

¹ Global Innovation Index: comparison with 2019; Global Fintech Index: comparison with 2020; given availability.

² Colors indicate relative ranking among the BRICS countries from green (best rank) to red (worst rank).

³ Identical scores (e.g. China = India = 87%) are shown as the same rank.

⁴ The highest-ranking cities of the BRICS countries are Moscow, São Paulo, New Delhi (Findexable)/Mumbai (IFZ), Hong Kong and Cape Town.

Note: BRICS stands for Brazil, Russia, India, China and South Africa.

⁵ And of many other upper-middle-income countries not shown in the table.

room for improvement and catch-up with the highest-ranking, mostly high-income, countries. The country's recent progress in innovation and competitiveness rankings has been more limited than in broader “doing business” or fintech indices (see last column of table 1)⁶.

Note that, beyond indices and rankings, Russia is one of only few countries globally that has its own information and communications technology (ICT) champions. For instance, the search engine of Yandex is nearly as popular as Google. The social media platform VK belonging to VK Company⁷ (VK) is more popular than Facebook/Meta⁸. Wildberries is Russia's leading enterprise in e-commerce, followed by Ozon, whereas in many other countries Amazon is the undisputed leader. Kaspersky Lab is the local no. 1 for cybersecurity services (Collman, 2021; Epifanova and Dietrich, 2022).

1.2 Reaching digital sovereignty – an important goal of Russia's government

In advocating digital transformation, the Russian government pursues different goals. Among other things, it wants to foster economic development and efficiency, but for geopolitical reasons it also strives for digital sovereignty. The term “digital sovereignty” has recently gained importance in policy discussions, but its interpretation varies. Germany, for instance, has put the emphasis on self-determination in shaping the digital transformation. For Russia, as Litvinenko (2021) argues, digital sovereignty is about controlling the flow of data and discourse within Russia.

This “control motive” ties in with Russia's legislation on the internet becoming ever more restrictive, which, according to researchers, started around the political protests of 2011–12, in which the internet and social media played an important role (Litvinenko, 2021; Epifanova and Dietrich, 2022). Legislation passed in the last decade⁹ – for instance, the heavily criticized “sovereign internet law” in 2019 – has aimed to increase the Russian government's ability to monitor and control the data flow within Russia. Such legislation has also extended to and affected the operations of international big tech companies such as Google or Facebook/Meta in Russia (Ilyushina et al., 2019; Epifanova and Dietrich, 2022). Russia's government has successively built – and repeatedly used – the technological and legal tools to fine or even (temporarily) ban these companies from the Russian market if they failed to comply with Russian laws, e.g. related to storing data on Russian territory or establishing representative offices in Russia (AFP, 2021; Seddon, 2021). Since the start of the war against Ukraine, Russia has further tightened its control over information spread in Russia (Barker and Tiirmaa-Klaar, 2022)¹⁰.

Also, while promoting national ICT champions and solutions, the Russian government has also taken action to maintain some control over these ICT companies,

⁶ However, it is difficult to compare and interpret these indices over time, as both methodologies and samples change and the indices mostly measure relative and not absolute progress.

⁷ Formerly known as Mail.ru Group – a rebranding to VK occurred in October 2021.

⁸ According to VK's Q4 2021 investor presentation, the VK social network had 72.5 million monthly active users, while Statista.com reported that Facebook had roughly 66 million users in Russia before the invasion. This figure does not include WhatsApp and Instagram, which also belong to Meta and had large active user bases before the invasion.

⁹ See Litvinenko (2021) for a detailed discussion of the origins and evolution of the Russian government's increasingly strict legislation and control of the internet in Russia.

¹⁰ Note that EU countries have also closed Russian websites and banned Russian TV channels.

some of which are internationally active and/or incorporated. For instance, in December 2021, entities affiliated with state-owned Gazprom acquired a controlling stake in VK Company, which is listed on the London stock exchange and owns Russia's largest social media platform VK (Epifanova and Dietrich, 2022). In 2019, Yandex agreed to adapt its governance structures, de facto guaranteeing that it remains under Russian control¹¹, even though Yandex is listed on Nasdaq, incorporated in the Netherlands and operates on global markets (Seddon, 2019).¹²

Moreover, the “control motive” also translates into the Russian government's aim to become less technologically dependent on other countries, particularly the USA. Thus, instead of simply promoting high-quality ICT services regardless of their origin, the Russian government has in many instances favored national solutions.

In this context, the aim to innovate and modernize has occasionally clashed with the aim to control and foster national solutions. Innovation tends to benefit from open and unrestricted cross-border competition and exchanges of information, products and services. This contrasts with action taken to foster digital sovereignty, such as tightening control of the internet, or with other measures meant to restrict the exchange of information or access to technology. For instance, Russia has obliged its national ICT champions to preinstall national versions of apps on mobile phones sold in Russia (Seddon, 2021), while simultaneously tightening legislation on foreign big techs. Ever stricter controls and monitoring of internet traffic and related regulations have made it more difficult and unattractive for foreign big techs to expand their offers in Russia, and has even pushed some companies out of the market. Such action can reduce the choices available to Russian consumers, some of whom might want to use services not affiliated with the Russian government.

Another example in this context is import substitution. Governments tend to resort to it to promote national firms and industry development. Yet, import substitution can come at the cost of – at least initially – using products and services that are of lower quality and/or cost more than available foreign alternatives – the typical infant industry dilemma. The Russian government has also used import substitution to promote national tech industries. For instance, it decided that only domestic systems and software were to be used to build Russia's 5G infrastructure. The government thus awarded a contract to state-owned Rostec, even though up to that point Russia had almost fully relied on telecommunications imports and Russian companies lack experience in the mass production of 5G equipment (Epifanova and Dietrich, 2022). Such import substitution is risky given that the 5G infrastructure is critical for operating and developing innovative services.

2 Border between technology and finance is blurring in Russia

What has certainly fueled the rise of Russian fintechs are (1) the supportive stance of both the Russian government and regulators coupled with (2) investments and initiatives to promote domestic ICT developments and (3) a cautious stance toward foreign big techs. At the same time, the government's drive for digital sovereignty may have weighed on innovations and fintechs overall. As the Russian financial

¹¹ Between 2009 and 2019, Sberbank held a “golden share” in Yandex, which allowed Sberbank to effectively veto transactions involving more than 25% of Yandex's stocks.

¹² We refer to these companies as Russian tech firms throughout the study given their history and influence structures, even though some are not incorporated in Russia. This also seems to be in line with market perceptions and actions taken by these firms after the start of the war (see section 3).

market has started to increasingly use platforms and digital ecosystems¹³, the border between tech companies and financial institutions has become blurred.

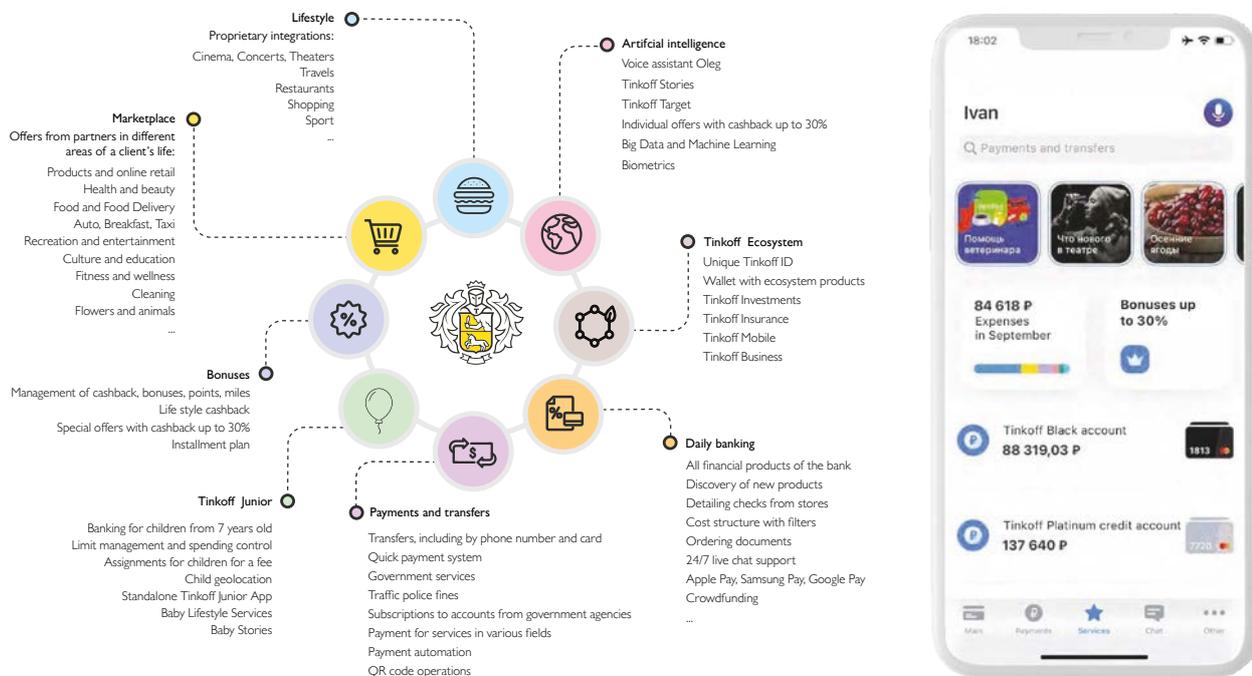
2.1 Large fintech companies launch digital ecosystems

For finance and banking in Russia, the emergence of digital ecosystems has been a two-way street: large Russian tech companies have moved into finance and financial intermediaries have started to diversify. Both have been creating digital ecosystems that offer a multitude of services to customers, including financial services (see figure 1 for an example).

Similar to other countries, large tech players in Russia have expanded into finance. A case in point is Yandex, which after a decade-long partnership with Sberbank, which soured, finally acquired Acropol Bank in July 2021. In August 2021, Yandex.Market started a partnership with Tinkoff Bank to offer loans to businesses selling on the platform. Following Chinese examples (e.g. WeChat/Tencent or Alibaba App), VK recently launched a “super app” for private and work purposes, which also includes its VK pay services. VK currently largely partners with financial institutions, e.g. Chinese banks and Sberbank, to offer financial services. Other firms that have started expanding their offerings and diversifying toward financial services are MTS (core business: telecommunications) and Ozon and Wildberries (core business: e-commerce; both recently acquired banks). In table 2, the firms discussed in this section are marked in bold.

Figure 1

Example of a digital ecosystem: Tinkoff Super App ecosystem



Source: Tinkoff (2021).

¹³ See footnote 4 for definitions.

Table 2

Selected Russian banks by size and owner¹

Rank by total assets	Name of bank	Approximate market share (%)	Total assets (EUR million)	Immediate parent/global ultimate owner	Country of ultimate owner
1	Sberbank of Russia	34.0	399,879.616	Ministerstvo Finansov Rossiiskoi Federatsii/ Russian government	RU
2	VTB	17.0	200,128.364	Federal Agency for State and Property Management/ Russian government	RU
3	Gazprombank	7.1	83,071.450	Federal Agency for State and Property Management/ Russian government	RU
4	Alfa-Bank	4.4	51,878.333	AB Holding/ABH Holdings	RU
5	Otkritie Financial Corporation	3.3	38,295.997	Central Bank of the Russian Federation/ Russian government	RU
6	Russian Agricultural Bank OJSC	3.6	42,136.451	Federal Agency for State and Property Management/ Russian government	RU
7	Credit Bank of Moscow	2.7	32,194.662	Rossum Concern/Avdeev Roman Ivanovich	RU
8	Promsvyazbank	2.6	30,961.255	Federal Agency for State and Property Management/ Russian government	RU
9	AO Raiffeisenbank	1.4	16,246.098	Raiffeisenbank International AG	AT
10	UniCredit Bank AO	1.2	14,300.739	UniCredit SpA	IT
11	Rosbank	1.3	15,117.462	Interros Capital (pre-war: Société Générale)	RU
12	Sovcombank OJSC	1.4	16,363.088	n.a./Sovcombank OJSC	RU
13	DOM.RF JSC	1.2	14,691.204	Federal Agency for State and Property Management/ Russian government	RU
14	Bank Rossiya OAO	1.2	13,575.850	Bank Rossiya OAO	RU
15	Bank Saint Petersburg PJSC	0.7	8,077.445	Bank Saint Petersburg PJSC	RU
16	SMP Bank LLC	0.6	7,540.419	SMP Bank LLC	RU
17	Tinkoff Bank	0.8	9,478.955	TSC Group Holding PLC	CY
...					
37	OJSC MTS Bank	0.2	2,375.607	Mobile Telesystems B.V./Mobile Telesystems PJSC	RU
...					
274	LLC Ozon Bank*	0.0	4.655	Internet Resheniya OOO (trades as Ozon) acquired Onei Bank OOO in 2021	RU
...					
313	Yandex Bank JSC* (previously Akropol Bank)	0.0	13.713	Yandeks.Market Lab/Yandex N.V.	NL
...					
356	Wildberry Bank LLC*	0.0	7.749	Bakalchuk Tatyana Vladimirovna	RU

Source: BankFocus Bureau van Dijk (BvD), Central Bank of the Russian Federation.

¹ Banks discussed in section 2.1 are marked in bold.

Note: Information on banks from BvD on consolidated level for 2020; if unconsolidated; bank name marked with *. Data as reported by BvD; differences between 2020 consolidated total assets and the rank could stem from the data point and consolidation method underlying the country ranking. Market share in % is an approximation using total assets of monetary financial institutions (MFIs) as reported by the Central Bank of the Russian Federation. Given rapid shareholder and ownership changes (see section 3), the table may not contain all recent changes.

Interestingly, some Russian banks have expanded into technologies more aggressively than their peers in other countries.¹⁴ First and foremost, Russia's largest bank, Sberbank, rebranded itself as "Sber" in 2020, and announced its aim to become a major consumer technology company. In the first half of 2021, Sberbank invested about USD 1 billion toward this aim, e.g. via its research labs dealing, among other things, with robotics, blockchain and artificial intelligence (AI) and via acquisitions¹⁵. Note that Sberbank has been one of the main drivers of AI development in

¹⁴ Even though investments in new technologies and other areas have become more common also in financial industries of other jurisdictions.

¹⁵ See, for instance, *Acquisitions by Sberbank* | Tracxn.

Russia (The Economist, 2022b). On top of this, Sberbank has created its own ecosystem, expanding into business areas where Yandex and VK have been active for years. Pre-invasion, Sberbank's target was to earn a particular share of its net operating income from its nonbank ecosystem holdings, namely 5% by 2023 and around 30% by 2030.¹⁶ Another bank working hard on building a diversified ecosystem is Tinkoff Bank, Russia's fast-growing largest digital bank. Founded in 2006 and following a rapid expansion, it is now Russia's third-largest retail bank.¹⁷ Tinkoff Bank was listed as a systemically important financial institution by the CBR in October 2021. In December 2019, it launched what it called "Europe's first Super App," which includes a broad range of financial, leisure and lifestyle services offered by Tinkoff and its partners (see figure 1).¹⁸ Russia's Digital Development and Communications Ministry lists Tinkoff Bank and several of its subsidiaries as information technology companies (Interfax, 2022). VTB, Russia's second-largest bank, has likewise announced its plan to expand into other key industries.

The digital ecosystems of Russian tech and financial companies are quite diverse because they have largely been built around the core business of the respective companies, be it financial services for banks, or social media, search engine data, e-commerce and the like in the case of tech companies. In 2021, the core business areas still accounted for the bulk of revenues, with newer business areas growing fast. Ecosystems also differ in that some companies diversify mostly by offering partner services, while others launch new services of their own. Most companies invest in advanced technologies, including AI and robotics, and they partner with or buy innovative start-ups, but the extent of such investments varies. The demand for digital ecosystem apps in Russia is strong: in the first eight months of 2021, Ozon's, Wildberries' and Sberbank's apps were downloaded 9 million times (in Russia) on major app stores, while the apps of VK, Yandex.Go (Yandex's taxi and delivery app) and Tinkoff were downloaded 7 million times (Tinkoff, 2021).¹⁹

2.2 Fintech digital ecosystems bring new regulatory challenges

In various countries, the rise of platforms and ecosystems offering financial services has attracted the attention of regulators, mostly as a result of big techs entering the financial sector. Big techs and platforms thrive on data analytics, network externalities and interwoven activities (abbreviated as DNA). Taken together, these activities create a positive feedback loop. Network externalities means that more users make a service more valuable for existing users. This leads to more data being generated that can be used in data analytics and commoditized and/or fed into additional services that, in turn, create more value for users of the platform or ecosystem. This business model gives rise to specific benefits and risks (Bank for International Settlements, 2019; Zamil and Lawson, 2022).²⁰

¹⁶ See, for instance, Sberbank's Investor Day Presentation "Strategy 2023": *Презентация PowerPoint (sberbank.com)*.

¹⁷ In terms of total assets, it is currently Russia's 17th-largest bank, according to rankings by BankFocus/Bureau van Dijk.

¹⁸ See *Tinkoff history: milestones in the Company's development (tinkoffgroup.com)*.

¹⁹ To put these figures into perspective: in the same period, TikTok's and Telegram's apps were downloaded 15 million times, WhatsApp and Instagram 10 million times and YouTube 3 million times.

²⁰ Please note that a comprehensive discussion of risks and benefits is beyond the scope of this study. Readers interested in learning more about this topic may consult the excellent reports cited in this section.

For consumers, platforms and digital ecosystems can have economic benefits, including a greater offer of goods and services, lower costs as well as ease of access, i.e. one login, many services. Businesses, in turn, may reach more customers without establishing costly branch networks; they may moreover share rules and expenditures, e.g. for customer support and logistics (CBR, 2021a). Platforms and digital ecosystems can also be important tools for promoting cross-sectoral digital transformation (World Bank, 2018). Over the past years, innovative financial services offered on digital ecosystems are likely to have contributed to the fast digitalization of finance in Russia.

However, the CBR (2021a) has also echoed concerns known from the broader international discussion on this topic. For reasons of scope, we only focus on selected key risks: (1) market concentration and domination, (2) deteriorating profitability of financial services, and (3) contagion and business risk.

First, market concentration is a major concern given that in the past platforms have occasionally shown very fast growth, not least due to the network effects implicit in their business models. Brits et al. (2021) argue that, beyond “standard” concerns about market power and competition, three types of concentration risk are particularly relevant for the financial sector: concentration of services, distribution and data. Concentration of services means that financial institutions offering more and more digital services might become dependent on a small set of providers of certain widely used technologies, such as cloud services, AI or software. This could lead to systemically important cyber risks. To address these risks, it will be necessary to revise regulations, e.g. regarding the definition and treatment of outsourcing and a greater focus on contractual relationships between financial and nonfinancial companies. As many companies based in sanctioning countries have restricted their business with Russian entities (see section 3), concentration of services might increase quickly in Russia given that the number of companies that may supply certain key technologies is limited.

Concentration of distribution refers to certain companies, platforms or ecosystems dominating the customer relationship, in particular the front end. This could hamper financial service providers’ ability to appropriately manage and assess risks relating to customers. Moreover, it could also have repercussions for trust along the financial value chain. If a “super app” or particular services offered within the app suffer from reputational damage, e.g. data leaks or misselling, this could spread to the broader ecosystem. This may damage the trust in the financial system regardless of whether the financial institution is involved in the affected ecosystem via a partnership model or as the provider of the front-end app (Brits et al., 2021).

Data concentration amplifies the risks of concentration of services and of distribution. In this context, it is also important to ensure that concentration of data does not lead to a buildup of entry barriers or to data misuse – for instance in the form of price discrimination or exclusion of high-risk groups from certain markets, such as insurance (Bank for International Settlements, 2019). In Russia, given the high share of state ownership and control, data could also be used by publicly owned firms for political purposes.

Second, ecosystem providers could start subsidizing their banking business with profits from other ecosystem services to gain more customers. Given the abovementioned DNA loop of digital ecosystems, banking services could function as a “hook” to generate more data that are then commoditized in other ways within

the ecosystem. This could undermine the profitability of stand-alone financial services, making it more difficult for financial institutions not involved in ecosystems to sustain their profitability (CBR, 2021b; Zamil and Lawson, 2022).

Third, another concern for the CBR (2021b) and other regulators are contagion and business risk, for instance, through concentrations of immobilized assets²¹. Such assets are mainly investments in equity and hybrid instruments, tangible assets and intangible assets. From a regulatory perspective, such assets entail risks for banks as they (1) do not create predictable cash flows, (2) cannot be used as collateral to obtain liquidity, (3) often have ill-defined valuations for lack of a liquid market for these assets and (4) occasionally, e.g. in the case of equity investments in start-ups, can be subject to high impairment risks. As such, they are usually subject to specific treatment when it comes to calculating regulatory capital. For instance, regarding investments in nonfinancial businesses, many countries worldwide have been much stricter than Russia. Some countries, e.g. the USA, have even completely banned investments by banks in nonfinancial businesses. In light of increased ecosystem investments, which are a particular form of immobilized assets, the CBR (2021d) has been working on tightening regulation on such assets in Russia.

Benefits and risks clearly vary across ecosystem providers and depend on the characteristics of the ecosystem. Companies pursuing partnership models may, for instance, be less prone to a concentration of immobilized assets on their balance sheets. Moreover, the abovementioned risks and benefits are not unique to Russia. They have also been discussed and analyzed in the context of other countries and have led to regulatory changes (e.g. Bank for International Settlements, 2019; Zamil and Lawson, 2022). However, in Russia, some risks, such as risks spilling over from financial services to the tech business and vice versa, may now be manifesting themselves faster than the CBR initially expected, amid technology-related and financial sanctions as well as the general economic turmoil that is hitting the different business areas of integrated fintech firms. Fortunately for Russia, ecosystem development is still in its infancy. Moreover, the CBR started to analyze risks early and was planning several new regulatory measures pre-invasion. The measures include regulating investments in immobilized assets, discussing an adjustment of the internal capital adequacy assessment process (ICAAP) and classifying banks operating large, diversified ecosystems as systemically important banks (CBR, 2021b).

3 Outlook for digital ecosystems has changed radically due to war in Ukraine and sanctions

In the following subsections, we discuss some recent challenges faced by digital ecosystem providers. The issues relate to international sanctions and the broader economic and geopolitical environment²². The changes are not only interesting from a regulatory perspective, but also from an economic perspective, given the considerable size and significance of the fintech conglomerates operating in the financial and technology sector of the Russian economy. Five years from now, Russia's digital ecosystems and their providers will look very different from what they would have looked like had there been no war in Ukraine.

²¹ The official term the CBR uses for these assets.

²² Given the rapidly changing environment and complexity of the topic, this section is necessarily incomplete. Please also note the cutoff date mentioned in footnote 4. Regarding sanctions, the interested reader could consult other sources listing sanctions, such as [Russia Sanctions Tracker](#) | Ashurst and [Russland FAQ: Informationen für Unternehmen - WKO.at](#) (in German only).

Note that at the time of writing, of the companies discussed in section 2.1 (Sberbank, VTB, Tinkoff Bank, Yandex, VK and MTS, Ozon and Wildberries), only VTB and Sberbank have been directly sanctioned by the EU or USA.²³ Companies not directly sanctioned are likely to have taken or take mitigating action as they might face sanctions in the future. Plus, such companies may be affected in other ways, e.g. via sanctions on individuals (leading to reorganizations of management) or sanctions on the import of certain goods and services into Russia (see below).

3.1 Financial sanctions likely to have largely indirect effects on digital ecosystems

Financial sanctions usually aim at restricting the ability of certain entities to obtain international financing or to access foreign assets. In the case of financial institutions, they can extend to financial transactions with entities of the sanctioning jurisdiction. Sanctions related to SWIFT, the global payment messaging system, may even severely limit all international financial transactions of the sanctioned institution. Indirectly, it also becomes more difficult for clients of the targeted financial institutions to effect financial transactions. As of mid-June, the USA and the EU have published long lists of financial and nonfinancial entities that are subject to financial sanctions. Ten banks have been excluded from SWIFT, namely Bank Otkritie, Novikombank, Promsvyazbank, Bank Rossiya, Sovcombank, Vnesheconombank (VEB), VTB Bank, Sberbank, Credit Bank of Moscow and Joint Stock Company Russian Agricultural Bank, i.e. JSC Rosselkhozbank.

Financial sanctions are impacting targeted entities through three major channels: (1) reduced access to funding from foreign entities and international capital markets, (2) transactions with foreigners and/or in foreign currencies are difficult or even impossible, which reduces the ability to offer goods or services abroad, and (3) confidence effects, also related to the impact of (1) and (2) on firms' available liquidity. All three effects combined have certainly weighed on Russian banks' foreign operations. For instance, in early March, European regulators ordered that Sberbank Europe be dissolved and its subsidiaries be dissolved or sold over liquidity concerns. Financial institutions face an additional important channel: deteriorating macroeconomic conditions lead to issues in the private sector that lower the asset quality on bank balance sheets.²⁴

However, while financial sanctions can be very powerful, several factors still mitigate their effects in Russia. For example, as long as some Russian banks have access to SWIFT, banks can transact with the rest of the world via the nonexcluded banks. Crypto assets have also been widely cited as a potential circumvention mechanism (see section 3.4). Finally, while SWIFT is an extremely important messaging system, it is not the only system. A case in point is a transaction system ("System for Transfer of Financial Messages"), which Russia developed in response to sanctions imposed in 2014 related to the conflict in Crimea, which it can now use to reroute national transactions.

As digital ecosystems in Russia are rooted in the domestic financial system, financial sanctions are likely to have only limited direct effects on the operation of

²³ Some companies, however, face sanctions from individual countries (e.g. Wildberries is on Poland's national sanctions list) or have seen certain services banned in selected countries (see, for example, Yandex/Estonia below).

²⁴ Based on existing research on financial sanctions and their macroeconomic effects, the current financial sanctions are likely to contribute to a deterioration of macroeconomic conditions in Russia (see e.g. Gurvich and Prilepskiy, 2015; Pestova and Mamonov, 2019).

the financial arms. By contrast, indirect effects are more substantial. Risks to digital ecosystems clearly also stem from the providers' liquidity and solvency position. Here, financial sanctions do play a role, but so do the overall loss in confidence associated with being sanctioned and its implications for obtaining financing, the collapse of stock market prices of listed companies and other issues, as discussed in the following sections.

3.2 Major revisions of business models due to sanctions (and risks)

Different types of sanctions (financial and nonfinancial, entity- and individual-based) have led to changes in organizational structures and business strategies. Because of sanctions it may become difficult or unattractive to develop certain services further. For instance, Sberbank announced in early June that it was closing SberGames, its gaming division, due to external restrictions for Russian developers on the global market (Bne IntelliNews, 2022a). In a similar vein, post-invasion, many international partnerships and expansion plans were terminated or stalled. Yandex, for example, decided to put several international expansion plans on hold, a number of partner companies have announced that they would end the partnership (Lee, 2022), and some countries, e.g. Estonia²⁵, have banned Yandex's services, also related to data concerns. Thus, sanctions may lead to ecosystems with less diverse or lower-quality service offers, which could make the ecosystems less attractive and profitable going forward.

Moreover, since the onset of the war, some digital ecosystem providers have had to radically re-evaluate their business model to salvage the future of their ecosystem development. As a case in point, the USA reported on April 6, 2022, that Sberbank and its subsidiaries would be put under full blocking sanctions²⁶. While being under sanctions might be less relevant for some subsidiaries/services (e.g. domestic taxi services or domestic financial transactions), it could be crucial for others (e.g. gaming, technology development). Possibly as a result of the sanctions, Sberbank announced in mid-May that it was selling several businesses belonging to its digital ecosystem, including SberCloud and its Speech Technology Center, to a relatively unknown company called Noviy Vozmozhnosti (Bne IntelliNews, 2022b).

Besides the sale or termination of business arms, several companies have also reported – sometimes multiple – management reshuffles or changes in shareholder structures as a result of sanctions on individuals or out of concerns regarding effective governance. Such organizational changes, particularly when forced and pushed through quickly, might imply increased risk for companies. For instance, TCS Group Holding, which owns Tinkoff Bank, announced in early April that it was “ring-fencing” its Russian business by transferring governance powers from the Board of Directors based in Cyprus to a Management Company controlled by the Russian management team of Tinkoff Bank²⁷. Some weeks later, after posting a critical tweet regarding the war in Ukraine, Oleg Tinkov, founder and important

²⁵ See *The government prohibits Yandex from offering taxi services in Estonia | Eesti Vabariigi Valitsus*.

²⁶ *Full blocking sanctions are the most severe financial sanctions in the USA, prohibiting US citizens, regardless of their location, from engaging in transactions with or for the benefit of targeted individuals and entities. Moreover, property belonging to such entities or individuals that is under control by US citizens is frozen.*

²⁷ See *Tinkoff news (tinkoffgroup.com)*.

shareholder of TCS Group, rushed through the sale of his share in the group. 35% of TCS Group were acquired by Interros, which is associated with Russian oligarch Vladimir Potanin. Tinkoff Bank announced that it would rebrand in 2022 and cease to use its old brand (Nechepurenko and Troianovski, 2022).

3.3 Impact of technology-related sanctions likely high

The third channel we cover in some depth are technology-related sanctions fintech companies with a core in tech are clearly most concerned about. Yandex, for instance, has already explicitly cited tech sanctions as a potentially severe medium-term obstacle to its operations.²⁸ Yet, tech sanctions also affect any Russian business wanting to provide innovative digital customer solutions and to develop and use cutting-edge technology.

Far-reaching tech sanctions were imposed on Russia by the USA, the EU and other jurisdictions, including Japan, South Korea, Taiwan and Singapore, all of which are major producers and exporters of advanced technological goods. China, which exports large volumes of high-tech goods²⁹, has not followed suit, however.

While sanctions vary somewhat across jurisdictions as to their precise wording and implementation, they are particularly strict for military end use or end users and dual-use goods. Also, Russia-wide sanctions apply to sensitive technologies that include microelectronics, telecommunications items, sensors, navigation equipment, avionics, marine equipment, and aircraft components. Moreover, the USA also imposed sanctions on goods produced outside the USA that use US software, technology or equipment.³⁰

Tech sanctions will bite because, despite some Russian success stories regarding technology development, Russia is nowhere near technological independence. In 2018, Russia's trade deficit (exports minus imports over total trade volume) in advanced technologies³¹ came to 69%, compared with 21% for the USA and 2.4% for the EU-27. Moreover, Russia's share in global patenting in advanced technologies was around 0.3% between 2016 and 2018, compared with around 22% in both the USA and the EU, and around 15% in China (European Commission, 2021). Discussing specific key ICT subindustries, Epifanova and Dietrich (2022) conclude that Russia's position in the hardware sector is quite weak, while its position regarding software is stronger, but also relies on Western companies. According to the authors, several multinational companies are critical for Russia's tech sector, e.g. SoftBank Group based in Japan, TSMC based in Taiwan, ASML based in the Netherlands or US (mobile) operating system and open-source repository providers such as Microsoft (Windows, GitHub), Apple (iOS) and Google (Android). All these companies' business in Russia is at least partially covered under the sanctions regime and some companies have joined large multinational private firms that have announced that they were voluntarily halting all new business in Russia.³² The

²⁸ See *Yandex — Company news — Yandex Provides Update on Impact of Current Developments*.

²⁹ See *High-technology exports (current US\$) - China, United States, Russian Federation, European Union | Data (worldbank.org)*.

³⁰ See e.g. *Russia's war on Ukraine: A sanctions timeline | PIIE (last accessed on April 14, 2022)*.

³¹ *Advanced technologies include advanced materials, advanced manufacturing, artificial intelligence, augmented and virtual reality, big data, blockchain, cloud technologies, connectivity, industrial biotechnology, the Internet of Things, micro and nanoelectronics, mobility, nanotechnology, photonics, robotics and security.*

³² *Currently, it is difficult to say whether this full suspension of business will be permanent or whether some business will resume in line with the imposed international sanctions.*

internet is a critical backbone of digital services, and its functioning in Russia might be negatively affected by foreign companies that provide, for instance, internet services and data transport pulling out of the country (Epifanova and Dietrich, 2022; Bateman, 2022).³³

Regarding the effectiveness of tech sanctions, it helps understand that achieving true technological independence is almost impossible for any country given the complexity of ICT products and integration of ICT supply chains. The use of semiconductors, a vital part of most modern electronic devices, is a prime example. Varas et al. (2021) pointed out that no other industry has the same high investment needs in R&D and capital expenditure. This has resulted in highly specialized and interdependent global supply chains that rely on free trade. According to Varas et al. (2021), there are more than 50 nodes across the semiconductor supply chain³⁴, where one region accounts for more than 65% of the global market share. This creates vulnerabilities; however, rebuilding the full supply chain on the regional level would require massive investments and result in much higher prices for semiconductors and the products that use them.

3.4 Sanctions need to be continuously updated to prevent circumvention

The Russian private and public sector will certainly attempt to evade sanctions and possibly succeed in some cases. For reasons of scope, we focus this section on tech sanctions, but its broader conclusions also apply to other international sanctions.

As to replacing sanctioned technologies, Russia may benefit from selective technological cooperations with China, which has also been targeted by Western sanctions and is making important efforts to reduce its technological vulnerability³⁵. In early February 2022, an official Sino-Russian friendship and cooperation declaration emphasized increased efforts to be put in the two countries' bilateral technological partnership stretching from e-commerce via cloud management to AI (Le Monde, 2022). In any case, the substitutability of many advanced tech products and services is limited, either because there are no substitutes available given the high concentration of certain ICT products or because a switch would only be possible by accepting a loss in quality, potentially compatibility, and thus performance. Nonetheless, President Putin issued a decree in mid-April 2022 that makes it compulsory to obtain permissions for imports of foreign hardware or software for use in Russia's information infrastructure. Moreover, the decree bans the use of foreign software in critical infrastructure from January 1, 2025 (Reuters, 2022).

Owing to some loopholes, it will still be possible to obtain sanctioned technologies or goods. For instance, the Russian Ministry of Industry and Trade has waved restrictions on parallel imports of certain foreign goods, meaning that it allows imports without the permission of the intellectual property owner. Ozon is reportedly

³³ Russia has been working on a "sovereign internet" that should be able to operate independently of the global internet. However, it is unclear if and when Russia could achieve this technologically very complex task (as we know little about the progress on this project).

³⁴ Russia and Ukraine are mostly relevant in the supply chains as providers of raw materials. Ukraine is a major supplier of neon gas, while Russia mostly supplies important metals, such as aluminum, nickel and copper. The geopolitical situation is therefore putting further pressure on the already stressed semiconductor supply chain.

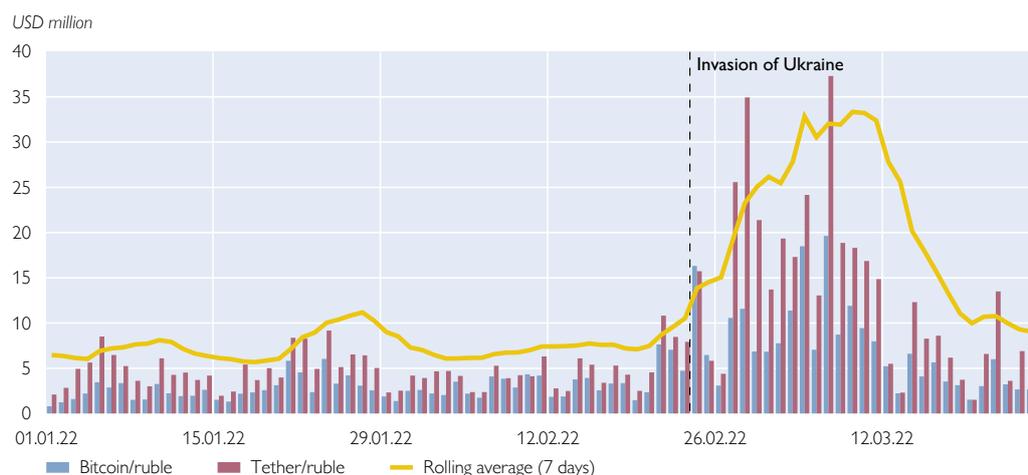
³⁵ China has been previously sanctioned by the West, e.g. under secondary sanctions, Huawei was cut off from access to sophisticated chips (semiconductors) using US technology. Consequently, as of end-January 2022, some big Chinese chipmakers – benefitting inter alia from lavish state subsidies – had reportedly established chip production lines "cleansed of US technology" (The Economist, 2022a).

already selling consumer electronics obtained via parallel imports³⁶. Another tool for evading sanctions that has been widely discussed in the media and by policy-makers are crypto assets. For instance, ECB President Christine Lagarde voiced her concerns about Russia's interest in the crypto economy as an instrument for bypassing sanctions, noting that the ECB was seeing a significant number of suspicious Russian crypto activities and was monitoring the situation (Look, 2022). After Russia's invasion of Ukraine, swaps of rubles to Tether and bitcoin increased markedly (see chart 1), probably a reaction to protect financial wealth amid the depreciating ruble exchange rate, inflation fears and sanctions.³⁷

However, various factors limit the ability to use crypto assets to evade sanctions in general, and tech sanctions in particular. First, the USA and the EU are trying to close loopholes in this area. For instance, the EU reacted by classifying crypto assets as "transferable securities," which implies that crypto assets should be treated like financial instruments with regard to sanctions. Note that this approach is not perfect; transferable securities are governed by the Markets in Financial Instruments Directive (MiFID II), which, however, allows for some differing classification approaches across EU member states. The Markets in Crypto-Assets Regulation (MiCA), which is expected to be finalized in 2022, is set to close certain regulatory gaps in this area. Second, large parts of the crypto economy, e.g. major exchanges and crypto service providers, have declared that they would comply with sanctions. Some exchanges even claimed to have gone beyond official sanctions by blocking transactions with all Russian banks (Dörner and Müller, 2022). While this is a positive sign for the effectiveness of sanctions, what complicates monitoring whether sanctions are honored and to what extent is the fact that across EU countries many players in the crypto economy are regulated differently, or not at all.

Chart 1

Volume of bitcoin and Tether swaps with ruble



Source: KAIKO.

³⁶ See *Ozon начал продавать электронику, ввезенную по параллельному импорту* - РИА Новости, 23.06.2022 (ria.ru).

³⁷ *Two weeks into the war, crypto trades reverted to their former level.*

Uncertain legal outlook for crypto assets in Russia

Russia's crypto economy is quite substantial, both in terms of mining and investments (CBR, 2021b). Regarding mining, a part of China's mining activities shifted to Russia after China's wide-ranging ban of crypto mining. As a result, Russia became the third-largest crypto mining country in the world. In late March 2022, the Russian Ministry of Energy called for an urgent legalization of mining and an introduction of regional energy quotas for bitcoin farms. The Ministry of Industry and Trade and the Ministry of Construction, Housing and Utilities followed up in April by also calling for an experimental legal mining regime.³⁸ Regarding investments, according to crypto ownership estimates published by TripleA³⁹, Ukraine and Russia are among the countries with the highest shares of the population holding crypto assets (around 12%, compared to e.g. 8% in the USA and 5% in the UK).

Until December 2021, Russia's official policy stance on the crypto economy was not quite clear. Some rejectionist indications for crypto mining and token issuance contrasted with signs of more lenient regulation. In January 2022, the CBR surprised the market by publishing a consultation paper on the trends, risks and regulation of crypto assets (CBR, 2022). In this paper, the CBR outlined that crypto assets should mainly be seen as high-risk assets, which lead to considerable systemic risks and are deeply ingrained in the money laundering business. The CBR recommended a complete ban of the crypto economy – mining, holding or investing in crypto assets, and especially using crypto assets as a means of payment.

The Russian government partially disagreed with the CBR's view, and it seems that the Russian Finance Ministry's more lenient view on crypto assets is prevailing: on February 18, 2022, the Russian Finance Ministry submitted a draft law on digital currency, which prohibits crypto assets as a method of payment but permits them as investment instruments and allows crypto exchanges to officially operate under strict customer identification and quality standards regimes. The Finance Ministry noted in its press release of February 21 that "proposals received from the Bank of Russia will be taken into account in further work on the draft law insofar as it does not contradict the approach of the Russian Ministry of Finance"⁴⁰. On April 8, the Finance Ministry announced that it had finalized the draft law and sent it to the government of the Russian Federation.

Third, the crypto economy is unlikely to provide enough liquidity to allow for a large-scale circumvention of sanctions, such as for larger international payments. Trades on the ruble spot market⁴¹ were, for instance, still roughly 13% larger in volume than all global bitcoin transactions, despite the steep rise in the volume of bitcoin transactions over the past years. This argument has less validity for smaller payments, e.g. the selective circumvention of restrictions on technological inputs or the use by private individuals to safeguard their wealth. Finally, all crypto transactions are permanently visible on blockchains, and may therefore be analyzed and tracked by authorities and analysts. This renders crypto transactions less suitable for circumventing sanctions, particularly for large transactions that are easily detectable, but also to a lesser extent for smaller payments, e.g. for buying technological goods.

³⁸ See <https://news.bitcoin.com/russian-finance-ministry-amends-bill-on-digital-currency-adds-crypto-mining-provisions/>.

³⁹ See *Global Cryptocurrency Ownership Data 2021 - TripleA* (triple-a.io).

⁴⁰ See Минфин России :: Пресс-центр :: Минфин России направил в Правительство России проект федерального закона «О цифровой валюте» (minfin.gov.ru).

⁴¹ CBR Database, https://www.cbr.ru/eng/hd_base/.

A dynamic tool, sanctions need to be constantly adapted as sanctioned entities find loopholes and ways to circumvent the existing sanctions. Export sanctions have, so far, had a severe, but not devastating impact on Russia's economy (see e.g. Chorzempa, 2022). If loopholes remain temporary and small, then the effect could intensify over time, as it will become more difficult for Russia to repair and replace essential ICT equipment, and for tech-dependent sectors to continue operating smoothly and develop innovative, cutting-edge solutions. This will ultimately damage Russia's economic power. Several other factors could likewise hamper the long-term outlook for Russia's technological advancement. As foreign companies are leaving Russia and new investments in Russia become riskier or are banned altogether, it will get more difficult to find partners for knowledge transfers, say via joint ventures. Given the economic consequences of the war, both the Russian public and private sector are likely to have to scale down the amount of funds they can spend on new investments. Chances are that well-educated Russians will be more motivated to emigrate for economic and political reasons, which could lead to skills shortages – although migrations following the Western sanctions and economic stagnation of 2014 did not stop Russia from achieving technological successes.

4 Summary and conclusions

In recent years, the Russian government has been pursuing a serious digital transformation agenda. It wants to foster economic development and efficiency, but – for geopolitical reasons – it also strives for digital sovereignty and control. On the one hand, Russia's experience with digital transformation illustrates how economic motives can clash with motives to nationalize and control. After all, innovation tends to benefit from specialization, competition and cooperation across borders. On the other hand, Russia's pursuit of greater technological independence has contributed to a variety of domestic ICT services and public infrastructures.

In addition, Russia's digital transformation has also contributed to rapid changes in the financial landscape. As to fintechs, the lines between tech firms and banks have been blurring fast, with digital ecosystems having become an important feature of the financial market. Pre-war Russia is therefore an interesting case study for a fast-changing financial landscape as well as the regulatory challenges that such a transformation entails. Compared to countries that undergo similar changes, Russia stands out as its largest bank, Sberbank, has been on the forefront of these developments.

Currently, the business models of Russia's large fintechs are being hit by international sanctions, and the firms have to grapple with a host of other issues related to the geopolitical context. Regarding technology-related sanctions, the Russian economy remains vulnerable, and particularly its tech and fintech firms. Despite its efforts to this effect, the Russian government has not yet managed to significantly reduce the country's technological dependence on foreign countries. The effect of sanctions is, however, somewhat mitigated by Russia having acquired experience in dealing with sanctions. It has built services and infrastructures, including payment systems, that are useful in the current context (Gagné Mapp, 2022). The Russian government is set to speed up its drive for digital sovereignty, but for lack of key technological inputs, this will become more difficult and costly. For advanced ICT products and services, which are highly specialized and complex, rebuilding regional supply chains would, for some technologies, require massive investments and might still result in costlier and inferior products (Varas et al., 2021). Overshadowed

by the war against Ukraine, Russia's fintech and ecosystem landscape will, over the next five years, develop differently from the path it had been on before the invasion. As large fintech firms play a crucial role in the Russian economy, adverse developments regarding their business should be watched closely.

The effectiveness of (tech) sanctions will play a critical role in determining the negative impact on the Russian economy over time. While sanctions are likely to be circumvented on a small scale, present possibilities for large-scale circumvention seem limited. For instance, using crypto assets to bypass sanctions on a larger scale is complicated by several factors. In any case, for sanctions to really bite, the sanctioning jurisdictions need to constantly monitor loopholes and evasion practices.

References

- AFP. 2021.** Russia fines Google for breaching data storage law. The Moscow Times. July 29.
- Bank for International Settlements. 2019.** Big tech in finance: opportunities and risks. In: BIS Annual Economic Report 2019. 55–79.
- Barker, T. and H. Tiirmaa-Klaar. 2022.** Deciphering Russia's wartime cyber campaign. Deutsche Gesellschaft für Auswärtige Politik (DGAP). Online commentary. March 16.
- Bateman, T. 2022.** How Russia could cut itself off from the global Internet, and why it probably won't. euronews.next. March 14.
- Bne IntelliNews. 2022a.** Russia's Sber moves to terminate SberGames division. June 9.
- Bne IntelliNews. 2022b.** Sber sells off its entire online ecosystem to obscure company. May 20.
- Brits, H., G. Cuijpers, N. Jonker, M. Lohuis, R. Roerink, C. ter Wal and A. Zwemstra. 2021.** Changing landscape, changing supervision: Developments in the relationship between BigTechs and financial institutions. De Nederlandsche Bank.
- CBR. 2021a.** Ecosystems: Regulatory Approaches – Consultative Report. Bank of Russia. April.
- CBR. 2021b.** Financial Stability Review Q2–Q3 2021. Bank of Russia.
- CBR. 2021c.** Priority directions of increasing financial inclusion in Russia 2022–2024.
- CBR. 2021d.** Regulating the risks of bank participation in ecosystems and investments in immobilized assets. Bank of Russia. Report for public consultation (only in Russian).
- CBR. 2022.** Cryptocurrencies: Trends, Risks, and Regulation. Bank of Russia.
- Chorzempa, M. 2022.** Export controls against Russia are working—with the help of China. Realtime Economic Issues Watch. Petersen Institute for International Economics. June 27.
- Collman, A. 2021.** Russia disconnected itself from the rest of the internet, a test of its new defense from cyber warfare, report says. In: Insider. July 23.
- Dörner, A. and M. Müller. 2022.** Von „Krypto als Rettungsleine“ bis zur Einstellung des Zahlungsverkehrs: So reagieren Kryptobörsen auf den Krieg. In: Handelsblatt. March 5.
- Epifanova, A. and P. Dietrich. 2022.** Russia's Quest for Digital Sovereignty. DGAP Analysis No. 1. February.
- Ernst & Young. 2019.** Global FinTech Adoption Index 2019 – As FinTech becomes the norm, you need to stand out from the crowd.
- European Commission. 2021.** Report on Russia: technological capacities and policy measures. Advanced Technologies for Industry – International reports.
- Gagné Mapp, M.-R. 2022.** Russian Fintechs and Sanctions. In: Irish Tech News. March 3.
- Gurvich, E. and I. Prilepskiy. 2015.** The impact of financial sanctions on the Russian economy. In: Russian Journal of Economics 1(4). 359–385.
- IFZ. 2021.** IFZ FinTech Study 2021 – An Overview of Swiss Fintech. Institute of Financial Services Zug (IFZ).

- Ilyushina, M., N. Hodge and H. Gold. 2019.** Russia rolls out its 'sovereign internet.' Is it building a digital Iron Curtain? CNN Business. November 1.
- Interfax. 2022.** Tinkoff Bank included in list of IT cos accredited by Russian ministry. June 8.
- Lee, D. 2022.** Yandex, considered 'Russia's Google', shaken and isolated by Putin's war. In: The Financial Times. March 4.
- Le Monde. 2022.** La guerre en Ukraine renforce la fragmentation du Web. April 29.
- Litvinenko, A. 2021.** Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty. In: Media and Communication 2021 9(4). 5–15.
- Look, C. 2022.** Lagarde Says Crypto Being Used to Evade Russian Sanctions. Bloomberg News. March 22.
- Melkadze, A. 2021.** FinTech in Russia – statistics & facts. Statista. August 23.
- Nechepurenko, I. and A. Troianovski. 2022.** Russian Tycoon Criticized Putin's War: Retribution Was Swift. In: NYTimes.com Feed. May 2.
- Pestova, A. and M. Mamonov. 2019.** Should we care? The economic effects of financial sanctions on the Russian economy. BOFIT Discussion Papers No. 13/2019.
- Reuters. 2022.** Russia to monitor foreign software purchases for state institutions – decree. March 30.
- Seddon, M. 2019.** Yandex agrees restructuring with Kremlin. In: The Financial Times. November 18.
- Seddon, M. 2021.** YouTube feels heat as Russia ramps up "digital sovereignty" drive. In: The Financial Times. May 22.
- Switzerland Global Enterprise. 2021.** Russian Fintech Industry: Opportunities for Swiss Companies – Industry Report.
- The Economist. 2022a.** China Inc and self-reliance – The techno-independence movement. February 26. 52–54.
- The Economist. 2022b.** Digital geopolitics – The Russian stack. February 19. 49–51.
- Tinkoff. 2021.** Lifestyle Banking – The core of the Tinkoff ecosystem. Presentation. September 30.
- Varas, A., R. Varadarajan, J. Goodrich and F. Yinug. 2021.** Strengthening the global semiconductor supply chain in an uncertain era. Semiconductor Industry Association (SIA) and Boston Consulting Group Report.
- World Bank. 2018.** Competing in the Digital Age – Policy Implications for the Russian Federation. International Bank for Reconstruction and Development / The World Bank.
- Zamil, R. and A. Lawson. 2022.** Gatekeeping the gatekeepers: when big techs and fintechs own banks – benefits, risks and policy options. BIS: FSI Insights No 39. January 20.