WHY SANCTIONS ARE NOT WORKING: HOW RUSSIA IS ADAPTING AND SURVIVING

By MICHAEL McMANUS

HJS Henry Jackson Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE FOR RUSSIA AND EURASIA STUDIES

June 2026

WHY SANCTIONS ARE NOT WORKING: HOW RUSSIA IS ADAPTING AND SURVIVING

By MICHAEL McMANUS

Published in 2026 by The Henry Jackson Society

The Henry Jackson Society
Millbank Tower
21-24 Millbank
London SW1P 4QP

Registered charity no. 1140489
Tel: +44 (0)20 7340 4520

www.henryjacksonsociety.org

Title: “WHY SANCTIONS ARE NOT WORKING:
HOW RUSSIA IS ADAPTING AND SURVIVING”
By Michael McManus

£9.95 where sold

Cover image: Close-up of surveillance cameras outside a Russian building flying the Russian flag by Спиридон Варфаламеев at pexels (https://www.pexels.com/photo/surveillance-russian-urban-camcorders-17157780/).

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE FOR RUSSIA AND EURASIA STUDIES

June 2026

About the Author

Michael McManus is the Director of Research at the Henry Jackson Society and oversees research at all our separate research centres. Prior to this, he worked as Director of Research at the Federation for American Immigration Reform (FAIR) in Washington D.C., where his work analysed the security and economic impacts of irregular migration, influencing legislation in the U.S. Senate and U.S. House. He also spoke as an expert witness at the Oklahoma State House. Michael has worked as an expert consultant on projects for the World Bank, European Commission, Deutsche Gesellschaft für Internationale Zusammenarbeit, and other high-profile clients. For over a decade, he worked at the European Parliament in Brussels, where he worked as an expert advisor on trade, security, and international development for multiple European Parliamentary groups. Michael provided analysis, research, and expert support during trade and aid negotiations between the EU and partner countries. These included some of the EU's biggest ever trade deals including the EU-Canada, EU-Japan, and EU-South Korea Free Trade Agreements. Michael was also involved in negotiating EU macrofinancial assistance to Ukraine following the invasion of Crimea, and in negotiations to provide EU macrofinancial to post-Arab Spring states.

Acknowledgments

I would like to thank Dr Helena Ivanov and Alexander Browder for their kind peer reviews of this paper. I also wish to thank Mykola Kuzmin and Ryan Stinger for their support in operations. In addition, I want to thank our fantastic interns Dimitri Kravets, Anastasia O'Reilly, Matthew Reynolds, and Angela Siby.

Contents

About the Author **2**
Acknowledgments **2**
About The Henry Jackson Society **4**
About the Centre for Russia and Eurasia Studies **4**
Foreword by The Lord Banner KC **5**
Executive Summary **7**
Sanctions Pressure 7
Autarky, Regime Survival, and Permanent Decoupling from Western Systems **9**
Sanctions Mitigation versus Sanctions Evasion **12**
Crypto and Sanctions Evasion **13**
Shadow Fleets, Oil Caps, and Teapot Refineries **15**
Hypothesis: Russia would turn to the shadow fleet to evade sanctions *15*
Teapot Refineries: How Chinese Companies Fund Russia's Oil Industry **19**
Alternative Banking Systems Compensate for Loss of SWIFT **20**
Hypothesis: Russia would see a decline in SWIFT following exclusion *20*
Adaptation 20
VISA, Mastercard, and Mir 22
External Trade Adaptation, A7, and A7A5 23
Digital and Technical Communication Alternatives **26**
Hypothesis: Russia would push Russian users away from western social media and into Russian-controlled alternative *26*
Russia and the Sovereign Internet **29**
Pushing Users into Russian Internet Alternatives **31**
Max 31
Yappy 32
RuTube 32
The Cost and Threat to the UK **33**
Conclusion **35**
Policy Recommendations **36**

About Us

DEMOCRACY | FREEDOM | HUMAN RIGHTS

About The Henry Jackson Society

The Henry Jackson Society is a think-tank and policy-shaping force that fights for the principles and alliances that keep societies free, working across borders and party lines to combat extremism, advance democracy and real human rights, and make a stand in an increasingly uncertain world. The Henry Jackson Society is a company limited by guarantee registered in England and Wales under company number 07465741 and a charity registered in England and Wales under registered charity number 1140489.

For more information, please see **www.henryjacksonsociety.org**.

CENTRE FOR RUSSIA AND EURASIA STUDIES

About the Centre for Russia and Eurasia Studies

The **Centre for Russia and Eurasia Studies** undertakes in-depth, analytically-focussed research into domestic and foreign policy issues in Russia and the other post-Soviet states. Established in 2010 as the Russia Studies Centre, the programme's geographical scope has widened since 2014, mirroring the high level of importance attached to the region.

Foreword by The Lord Banner KC

Following Russia's invasion of Ukraine, the free world came together in an almost unprecedented show of solidarity with Ukraine. The US, UK, EU, and other democratic powers imposed some of the most comprehensive sanctions ever imposed on Russia. These sanctions aimed to constrain the Russian economy, punish Russian political figures, and ultimately, undermine Russia's ability to fund its war against Ukraine.

But as this paper shows, despite our widespread sanctions, the ever-cunning Kremlin has devised ways to cope. This paper by the Henry Jackson Society demonstrates that Russia, despite being under constraint, has sadly managed to adapt, survive, and continue its aggression against the people of Ukraine.

Russia has spared no expense in adapting to sanctions. At home, it has built systems of banking and communication to offset its exclusion from western banking systems like SWIFT, and built its own versions of social media platforms to better spread Moscow's lies about the war. These domestic adaptations have allowed Russia to take the strain, minimize the cost of exclusion from western systems.

Overseas, Russia has sent its "shadow fleet" of unregistered and uninsured oil tankers across the world to sell oil in violation of western price caps. Organisations and individuals in third countries like China and Kyrgyzstan have enabled Russia to obtain equipment and parts in violation of trade sanctions. And with cryptocurrency, such as the Moscow-backed A7A5 stablecoin, Russia has deviously managed to route payments outside of western control and monitoring.

In short, western leaders hoped that sanctions would strangle Russia's economy and with it, the ability to project aggressive force against its neighbours. But Russia has survived. Ever since its illegal annexation of Crimea in 2014, Russia has prepared for the scenario of heavy sanctions. When the west imposed sanctions in 2022, Moscow scaled up its existing systems or introduced new ones to cope.

This paper makes a vital contribution to academics, policymakers, lawmakers, and security experts. Only by understanding how Russia has been able to soften the impact of sanctions can we better understand how to react. By doing so, we can better work with international partners to understand the loopholes and tactics used by the Kremlin, and then work to close them.

As the world's autocracies flex their muscles, the democratic world must be more ready than ever to defend our values. Part of this readiness includes being clear on what does and does not work in sanctions regimes, and how autocracies adapt and survive in the face of them. Sanctions send a powerful message, but that powerful message must have a tangible ability to impose costs and restrictions on the target.

I highly recommend this paper, and urge all those concerned about democracy, freedom, human rights, and national self-determination to read it. As the gallant people of Ukraine have shown, tyranny can be resisted. But tyranny would be that much easier to resist if it could not find a way to financially support its aggression against its neighbours. Moscow has shown it is possible to adapt and continue coercion under restraint. If we no not act, other tyrannies may copy, and the consequences will be disastrous.

The Lord Banner KC

Executive Summary

Sanctions imposed on Russia since its invasion of Ukraine have created significant constraints on its access to global communication, financial, and commercial systems. These sanctions have incentivised innovation and institution building, including new social media apps and payment networks that are beyond Western monitoring and control. In addition, the use of cryptocurrency and 'burner banks' have helped to disguise payment flows and maintain Russia's economy. Russia also takes advantage of illicit trade networks, such as shadow fleet oil sales. Together, these adaptations have produced a Kremlin-controlled digital and financial 'splinternet' ecosystem that weakens Western leverage and complicates sanctions enforcement. Consequently, Russian resilience be able weather the imposed sanctions more easily than originally envisaged, actually enhancing regime survival under such pressures. Moreover, this economic resilience allows Russia to financially support external coercion, for example against Ukraine and in its hybrid war on the West, while maintaining internal coercion strategies that detect and punish opposition inside Russia, such as surveillance and suppression of dissidents.

Sanctions Pressure

Vladimir Putin became president of Russia in 1999, succeeding the first post-Soviet president, Boris Yeltsin. Between 1999 and 2008, Russia was cautiously welcomed into the international community. The assumption was that Russia would be integrated into the Western-centred model of globalisation. However, relations began to cool as Russia targeted Estonia and Georgia in 2007 and 2008, respectively. In 2014, the annexation of Crimea and portions of eastern Ukraine triggered sanctions and escalated hostilities between Russia and the West. Yet it was Russia's full-scale invasion of Ukraine in February 2022 that was the decisive turning point. Russia has been effectively excluded from all major Western systems of payment and communication.

Western sanctions have caused various economic difficulties for Russia. The UK's Foreign, Commonwealth & Development Office estimates that up to June 2025, Russia losses due to sanctions totalled at least $450 billion [1] – equivalent to 25% of Russia's pre-war GDP. The total includes an estimated $154 billion in lost oil tax revenue and approximately $285 billion in frozen overseas Central Bank reserves. According to the Organization of Economic Complexity, Russian exports to Europe have fallen from $239 billion in 2021 to just $41.5 billion in 2024. [2]

At this point it is useful to distinguish between comprehensive and smart sanctions on nations. Comprehensive sanctions target the economy of an entire country, while smart sanctions target specific individuals or businesses. An example of comprehensive sanctions is Yugoslavia during the 1990s, which was subjected to a total trade embargo. Both imports and exports were sanctioned, and all Yugoslavian foreign assets were frozen. Comprehensive sanctions are used to apply broad pressure on both a government and its population to force changes. Although such sanctions are rapid to implement with powerful outcomes, they often impact ordinary citizens disproportionately. In contrast, smart sanctions are applied more granularly, for example against Muammar Gaddafi and members of his entourage in 2003. These were imposed due to alleged support for weapons of mass destruction, and were lifted when he agreed to cease development of such weapons. [3]

1 "Estimating the impact of sanctions on Russia's war efforts", UK Foreign, Commonwealth and Development Office, https://www.gov.uk/government/publications/estimating-the-impact-of-sanctions-on-russias-war-efforts.

2 "Russia (RUS) Exports, Imports, and Trade Partners", Observatory of Economic Complexity (OEC), https://oec.world/en/profile/country/rus?selector345id=2024.

3 "2003: Libya gives up chemical weapons", *BBC News*, 19 October, news.bbc.co.uk/onthisday/hi/dates/stories/december/19/newsid_4002000/4002441.stm.

The United States, European Union, and other allied countries have applied sanctions to Russia,[4] mostly in the form of smart sanctions aimed at oligarchs, political figures, and military commanders.[5] Therefore, the individuals targeted by these smart sanctions are those who have the most direct power over Russian state actions. By applying sanctions against such individuals, the end goal is to force them to enact policy changes and avoid applying pressure to ordinary Russians. Notably, although Russia has been constrained by these sanctions, the Putin regime has sought ways to ameliorate their impacts through parallel financial systems, illicit trade, cryptocurrency, and third-country assistance. By doing so, Russia has been able to preserve state revenue and economic capacity.

4 "Timeline – EU sanctions against Belarus", European Council/Council of the European Union, www.consilium.europa.eu/en/policies/sanctions-against-belarus/timeline-eu-sanctions-against-belarus/.

5 "Russia-related Sanctions", Office of Foreign Assets Control, US Treasury, https://ofac.treasury.gov/sanctions-programs-and-country-information/russia-related-sanctions.

Autarky, Regime Survival, and Permanent Decoupling from Western Systems

Sanctions invariably pose a challenge to regime survival in autocratic contexts. By restricting or blocking access to economic resources, payment systems, and financial services, political authority is undermined. The ensuing disruption can weaken the systems of financial patronage that are a feature of authoritarian states, as well as corrode the regime's ability to maintain everyday economic stability. Support for such regimes is mainly dependent on continued patronage to security and political elites, and partly on broader popular tolerance for economic instability. Thus, it is imperative for regimes under sanctions to rely on domestic ingenuity, informal market mechanisms, and the assistance of sympathetic or permissive third countries to create a sanctions-resilient resilient political ecosystem.

Russia, similar to all autocracies, places regime survival above all considerations. It is critical for the Kremlin to maintain domestic continuity. According to the US Congressional Research Service, much of Putin's popular legitimacy stems from the improved standard of living associated with his rule, in sharp contrast to the chaos and deprivation of the Yeltsin era.[6] Because Western sanctions can undermine the current national standard of living, slowly increasing political resentment to weaken Putin's grip on power, whether through sanctions mitigation or evasion, his ultimate goal is resilience: the regime's ability to maintain economic survival.

One critical feature of Russia's adaptation to post-2022 sanctions is the permeance of the imposed changes. The policies and platforms adopted by Russia in response to sanctions are not seen to be temporary reactive adaptations, only in place until a post-war normalisation and reintegration into Western systems can be realised. The sheer cost, scale, and reach of the adaptations speak to a permanent new order rather than emergency temporary measures. As an autocracy, Russia has a heightened ability to reallocate resources quickly, suppress attempts at transparency, and ruthlessly control any form of dissent. Hence, Russian systems are optimised for national control to enhance regime survivability under stress, whereas Western systems are optimised for global interoperability,

Several additional factors show that Russia's policy changes as responses to sanctions are more likely to be permanent as opposed to emergency or temporary measures. First, mobile payment applications and legal requirements for their use are clear signs of institutionalisation and thus permanence. Some of these apps were developed in the years leading up to the war, and war has made them permanent and mandatory. Russian legislation has made certain payment apps and payment systems mandatory for some services. Moreover, these new laws do not contain any sunset clauses, suggesting that the changes will be permanent.[7] Such creation of systems that are mandatory for key transactions and buttressed by institutions and legislation underlines this permanence.

Since 2008, with its overt aggression against Georgia and Estonia, Russia has positioned itself not as an aspiring member of the Western-dominated global system but as a revisionist state. Russian thinkers, such as Alexander Dugin and members of the influential 'Izborsky Club', have urged the Kremlin to pursue a hawkish stance toward Russian territorial expansion into parts of the former Soviet Union – especially Ukraine.[8] A regime pursuing territorial expansion of this kind would be aware of reprisals for this expansion, such as sanctions, and would prepare

6 "Russia: Domestic Politics and Economy", Congressional Research Service, 9 September 2020, www.congress.gov/crs_external_products/R/PDF/R46518/R46518.6.pdf.

7 "Federal Law of 24 July 2023 No. 369-FZ 'On Amendments to the Federal Law' 'On the National Payment System'", Russian Government, 24 July 2023, publication.pravo.gov.ru/Document/View/0001202307240049.

8 Juliette Faure, "What role did ideology play in triggering Russia's invasion of Ukraine?", The Russia Program at George Washington University, Online Papers No.8, 1 October 2023, www.therussiaprogram.org/onlinepaper-8.

for these reactions in advance. Indeed, certain Russian financial systems were built in 2014, strongly suggesting that Russia had a long-term goal of detaching from Western systems and was not simply reacting in panic to post-2022 sanctions by setting up its own.

Post-2014, and especially post-2022, Russia has sought to establish its own systems of communication and commerce. These allow Russia to effectively evade sanctions where its own systems were insufficient to mitigate their impact. [9] Russia increasingly pursues financial autarky via selective decoupling from Western-controlled systems and where possible, substitution of these systems with domestically controlled equivalents. While complete decoupling from the Western-dominated global system is almost impossible, Russia has identified where it is most able to assert domestic control. In areas where Russia can substitute Western systems with its own, Russia does so. In areas where Russia has not been able to effectively remove itself and provide a domestic equivalent, it simply violates sanctions through evasion tactics that use existing systems.

Russia's actions in adapting to sanctions can be located within the realm of autocratic adaptation. The adaptations are not completely distinct from coercive strategies, but are part of its coercive contest with the West. Russia's adaptations to current sanctions are broader than increasing resilience, they are designed to re-engineer its banking and communications systems to side-step the coercive mechanisms of the Western sanctions. Therefore, by allowing Russia to continue its economic and military operations, its adaptations are essentially forms of counter-coercion. As an autocracy, Russia has an adaptive advantage over democracies in that Russia has the ability to redistribute coercive costs, is comparatively more insulated from public pressure, has greater control over capital and resources. Such factors may be the reason for its relaxed attitude to illegal practises, such as sanctions evasion and money laundering.

In addition to its own policy changes and economical manoeuvres, Russia has received aid from third countries, most significantly China. China has functioned as a middleman, allowing Russia to obtain components and materials that it cannot purchase directly. Further, despite it being a democracy, India has continued to purchase Russian oil, taking advantage of the fact that Russia is not barred from selling oil, rather not permitted to sell it above a certain value. [10] Others actors are alleged to be helping Russia avoid sanctions; for example, companies in Central Asian countries also acting as middle men, with their own governments denying knowledge of their actions. [11] Even overseas Russian individuals have been accused of using European postal services to send banned materials to Russia, exploiting lighter controls on international mailing in some countries. [12]

In sum, through the combination of mandating the use of their own systems, layers of legislation, and the rhetoric around sovereignty, all strongly suggest Russia's post-sanctions adaptations are permanent. These actions are all underpinned by the timing of the measures, which were built years before the all-out war with Ukraine.

At the heart of the Russian adaptation to sanctions strategies, there are three main components: negation, deterrence, and enablement. In the case of negation, Russian adaptations permit

9 Dabrowski M. and Avdasheva S., "Sanctions and Forces Driving to Autarky", The Contemporary Russian Economy, Springer Nature Link, 1 January 2023, pp.271-288, www.link.springer.com/chapter/10.1007/978-3-031-17382-0_14.

10 "No sanctions on buying oil from Russia", *Economic Times (India)*, 26 September 2025, www.economictimes.indiatimes.com/industry/energy/oil-gas/no-sanctions-on-buying-oil-from-russia-hardeep-puri/articleshow/124158467.cms?from=mdr&utm_.

11 "Authorities Rail Against Use of Kazakhstan in Circumventing International Sanctions Against Russia", *The Times of Central Asia*, 25 October 2024, www.timesca.com/authorities-rail-against-use-of-kazakhstan-in-circumventing-international-sanctions-against-russia/.

12 "Russia uses 'shadow mail' postal system to bypass EU sanctions, report reveals", Euronews, 29 January 2026, www.euronews.com/2026/01/29/russia-uses-shadow-mail-postal-system-to-bypass-eu-sanctions-report-reveals.

it to negate the economic pain caused by sanctions and thus deny the ability of sanctions to compel behavioural changes. Deterrence allows Russia to portray itself as being unbowed by sanctions pressure, thus sending the message that the current measures have failed, therefore deterring the prospect of future sanctions. Enablement is arguably the most important component, as sanctions adaptations allow Russia to continue its coercive behaviour that triggered the sanctions in the first place.

Table 1: Main Mechanisms of Russian Adaptation to Coercive Sanctions Pressure.

Negation	Deterrence	Enablement
Sanctions fail to compel change in the targeted country.	Economic and military endurance in the face of sanctions signals futility of future sanctions.	Allows uninterrupted coercion across domains.

Sanctions Mitigation versus Sanctions Evasion

There are important differences in how sanctioned individuals and states react. In the case of sanctions mitigation, the sanctioned party takes steps to mitigate the impact of sanctions, yet does so within the bounds of the law. An example of sanctions mitigation is being barred from payment system A but not payment system B; therefore the sanctioned party subsequently operates via payment system B. In sanctions evasion, the sanctioned party attempts to circumvent the ban by using illegal activities. For example, a sanctioned party continues using system A using fraudulent means. Russia has used a combination of both sanctions mitigation and evasion to try and reduce the damage of Western sanctions.

Crypto and Sanctions Evasion

An emerging and effective means of evading sanctions is the use of cryptocurrency, which is digital and borderless, and therefore does not require a bank to process transactions. While generally visible, transactions are tied to wallet addresses but not verifiable identities. The fact that cryptocurrencies are spread across multiple jurisdictions with different 'know your customer' laws and sanctions enforcement rules only increases both the appeal of this route and the difficulty in implementing sanctions.

Russia has energetically embraced cryptocurrency as a means of evading sanctions. The country has an unusually high abundance of technical expertise due to its prioritisation of STEM studies relative to other countries.[13] As such, Russia has been able to quickly use and develop a cryptocurrency ecosystem. Given the country's isolation from traditional banking and payment networks, and the speed and secrecy afforded by cryptocurrency use, the Kremlin has enthusiastically leaned into the payment ecosystem afforded by cryptocurrency.

In a typical sanctions-evasion scenario, Russia first seeks to access an 'on-ramp,' i.e. a mechanism that is used to convert traditional currency, such as the US dollar into a cryptocurrency. A typical step to perform this conversion uses a crypto-exchange platform or a broker. Once the fiat currency has been exchanged into cryptocurrency, the funds can then be transferred overseas, outside of traditional payment systems like SWIFT. To further ensure secrecy, the funds are subjected to 'layering', a process that passes the funds between different crypto wallets. Although this does not make the transactions invisible, it complicates attempts to trace the funds. Once layering is complete, the crypto funds reach the service provider, which then converts them into a fiat currency, such as the US dollar or Chinese Yuan.

Layering is facilitated by decentralised exchanges (DEX), platforms where multiple users place crypto funds into the same pool, which then sends funds back in a different type of cryptocurrency with an equal market value. They are principally designed to allow trading, and are fully transparent. Critically, transactions are fully transparent on the blockchain and there are no attempts to obscure the transaction history. Decentralised mixing services perform a similar role. Users deposit funds which are pooled, and then withdrawn at a later date. Unlike the decentralised exchange, a decentralised mixing service is explicitly designed to prevent blockchain tracing. An analogy would be a pot into which 100 users place a £20 note, the pot is stirred then a £20 note is taken out by each user. It would be impossible to tell which note was originally yours, but this would not matter as you still got £20. However, by mixing your money with others, somebody looking for the original note would be unable to tell who it had originally belonged to. By doing this using cryptocurrencies (and for significantly larger amounts) the ability of law enforcement to detect the origin and owners of assets is massively reduced.

An example of a decentralised mixing service is 'Tornado Cash', which was blacklisted by the US Department of the Treasury in August 2022 (although this was overturned in March 2025). Although there were concerns about Tornado Cash being used for nefarious reasons, the reason for it being delisted was the fact that, because the exchange was decentralised and open source, it was not a legal entity therefore could not be sanctioned.[14] In August 2025, the founder of Tornado Cash was convicted of operating an unlicensed money transmitting

[13] Michael McManus, "Catching Sandworm: How Russia Wages Cyberwarfare Against Ukraine and NATO", The Henry Jackson Society, January 2026, www.henryjacksonsociety.org/publications/catching-sandworm/.

[14] "Fifth Circuit reverses U.S. sanctions against cryptocurrency mixer Tornado Cash", *American Bankers Association Journal*, 3 January 2025, www.bankingjournal.aba.com/2025/01/fifth-circuit-reverses-u-s-sanctions-against-cryptocurrency-mixer-tornado-cash/.

business. [15] However, Tornado Cash is not the only DEX of its kind, so nefarious actors can make use of multiple similar platforms. The legal gaps in the regulation of DEX have not gone unnoticed by Russia.

There is some overlap between a decentralised exchange and a decentralised mixing service: both can have complex tracing routines, but only the decentralised mixing service intentionally obfuscates the process. In a decentralised exchange, users can swap assets through means of shared liquidity pools, which have the unintentional effect of complicating tracing due to breaking unit-level continuity between the input and output assets.

Table 2: Comparison Between Features of Decentralised Exchanges and Decentralised Mixing Services for Cryptocurrency.

	Decentralised Exchange (DEX)	Decentralised Mixing Service
Primary Purpose	Trading	Obscuring trade origins
Assets Inputs/ Outputs	Different assets (e.g. BTC and ETH)	Same assets
Rationale	Market exchange	Privacy/Anonymity
On-Chain Transparency	High	Low by design

China has been especially impacted by sanctions on Russia. This is especially true given the level of pre-sanctions trade that had existed between the two countries, and the imposition of secondary sanctions that increase the risk when trading in dollars with a sanctioned country like Russia. While China is hostile to the West, the Chinese economy could not function without the ability to trade in dollars and cannot risk falling foul of US sanctions for doing so.

To circumvent these secondary sanctions, China has made use of so-called ‘burner banks’. The term burner is a play on the idea of a ‘burner phone’, a device intended to obfuscate ownership and that can be discarded once used. Burner banks are financial institutions that are set up in countries with weak or permissive jurisdictions to facilitate China–Russia trade, and are quickly shut down once trade transactions have been completed. [16] At the heart of sanctions monitoring and enforcement are identifiable permanent links; however, if the banks facilitating illicit trades are quickly shut down, then the investigation cannot succeed.

[15] “Founder Of Tornado Cash Crypto Mixing Service Convicted Of Knowingly Transmitting Criminal Proceeds”, United States Attorney’s Office, Southern District of New York, 6 August 2025, www.justice.gov/usao-sdny/pr/founder-tornado-cash-crypto-mixing-service-convicted-knowingly-transmitting-criminal.

[16] Piotr Dzierżanowski and Marcin Przychodniak, “China’s Economic Support for Russia Since the Full-Scale Invasion of Ukraine”, The Polish Institute of International Affairs, 11 February 2025, www.pism.pl/publikacje/chinas-economic-support-for-russia-since-the-full-scale-invasion-of-ukraine.

Figure 1: Russia uses roubles to buy a crypto coin to pay for goods from a Chinese supplier. The Chinese supplier takes payment in crypto via a DEX, which obfuscates the origins of the sender and thus allows plausible deniability for sanctions breaking. [17]

[17] “Russia leans on cryptocurrencies for oil trade, sources say”, *Reuters*, 14 March 2025, www.reuters.com/business/energy/russia-leans-cryptocurrencies-oil-trade-sources-say-2025-03-14/. Infographic produced by Microsoft Co-Pilot.

Shadow Fleets, Oil Caps, and Teapot Refineries

Russia's main source of income is petrochemicals exports. In 2021, Russia exported $228 billion in petrochemicals exports, accounting for 47% of the country's foreign exports.[18]

As Europe tightened sanctions on Russian oil, this formerly lucrative market began to shrink. This meant that access to the much-needed foreign currency, with which Russia's customers pay for services and which is vital to Russia's ability to financially prosecute its war in Ukraine, was greatly reduced.

One factor further aggravating Russian oil revenue is the price cap. In 2022, the EU, G7, and Australia imposed a cap of $60 per barrel on Russian oil sales, meaning countries would not be permitted to pay more than $60 per barrel. In exchange for compliance with this price cap, ships carrying Russian oil were permitted to use Western shipping, financial services, and insurance. Subsequently, the price cap was lowered to $47 a barrel in July 2025, and the technique appears to be working. Russia received just $41 per barrel in December 2025, and for oil produced in the Urals this figure was as low as $38 per barrel.[19]

Russia's oil industry has been further hit by strikes on its oil industry infrastructure by Ukrainian drones. To counter the price caps, Moscow turned to the 'shadow fleet', a network of unregistered ships used to transport Russian oil. By misrepresenting their origins, ships in the shadow fleet are used to evade sanctions.

One technique used by the shadow fleet is the 'ship-to-ship' transfer of oil. This technique involves two ships drawing alongside each other, usually in a location that is remote to avoid detection, and the ships' automatic identification system (AIS, used to show where the ship is geographically located) is turned off. Disabling the AIS allows the ship to disguise its route, vital for discrete meetings. The oil is then transferred from a sanctioned vessel to an unsanctioned vessel, which can then enter a port and sell it avoiding current price caps. During the ship-to-ship transfer, paperwork can be exchanged, generally with the aim of misrepresenting the origin of the oil, again as a means of evading sanctions.

Hypothesis: Russia would turn to the shadow fleet to evade sanctions

To establish if and to what extent Russia was turning to the shadow fleet to help dodge sanctions, data on shadow fleet oil shipment activity were compiled.[20] These data include both crude oil and other oil products. If Russia was using the shadow fleet to adapt to a sanctions-constrained environment, then an increase in shadow fleet activity would be expected. The results are shown in Figure 2.

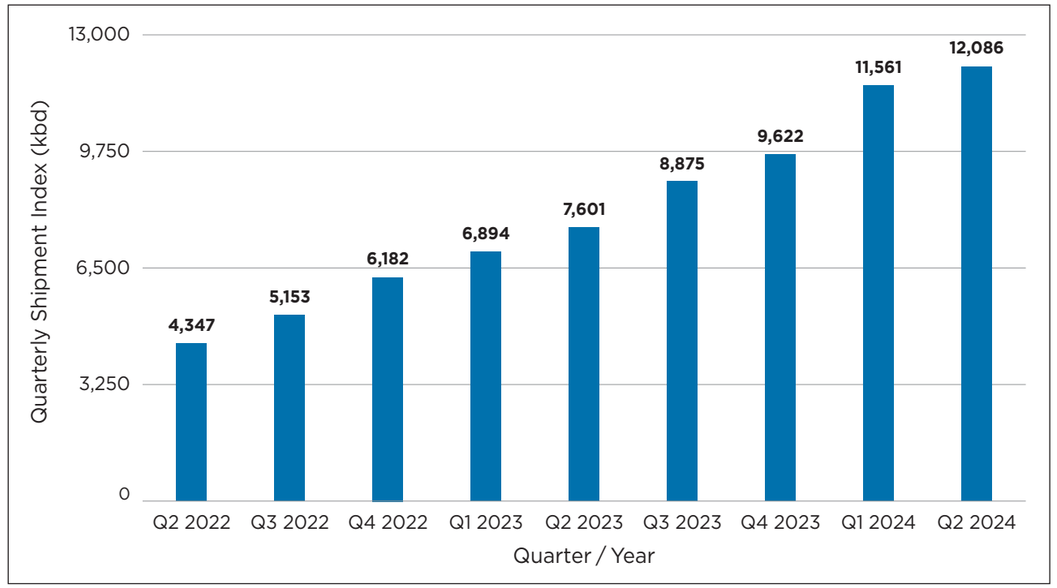
Trading cryptocurrency allows Russia and China to maintain their commercial links in spite of sanctions. Stablecoins enable entities to hold and transfer dollar-linked values outside of the internationally regulated banking system. A common pathway is when China purchases Russian oil, paying RMB to a middleman using an offshore account. The middleman then converts this RMB to cryptocurrency, before transferring the cryptocurrency to a Russian account where it is converted back to its equivalent in Rubles.

[18] "Russia Exports, Imports, and Trade Partners", Organization of Economic Complexity, https://oec.world/en/profile/country/rus?selector345id=2021.

[19] Benjamin Hilgenstock, Yuliia Pavytska and Matvii Talalaievskyi, "Spending Cuts Keep Budget On Target; Russian Oil Prices Continue To Plunge", KSE Institute, PowerPoint Presentation, January 2026, https://kse.ua/wp-content/uploads/2026/01/Chartbook_January2026.pdf.

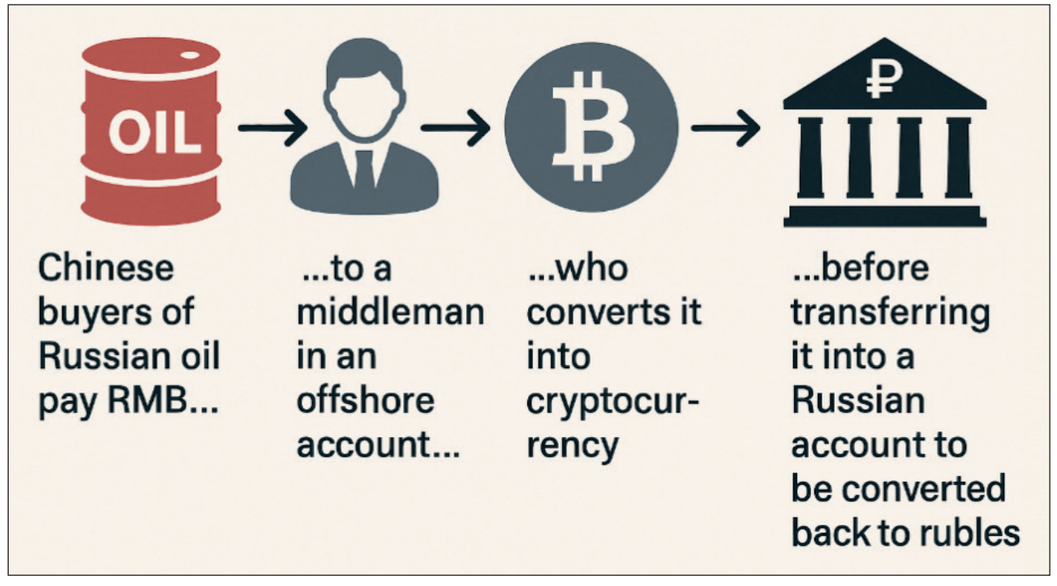
[20] Figure calculated based on KSE Institute (2024), using data from Equasis, IG P&I Clubs, and Kpler, then arranged into quarterly periods.

Figure 2: Quarterly Shadow Fleet Oil Shipments (thousand barrels per day/kdb).



Sources: Author's calculations based on KSE Institute (2024),[21] using data from Equasis, IG P&I Clubs, and Kpler.[22] Chart by HJS.

Figure 3: Illustration of how China uses bitcoin and offshore accounts to help Russia avoid sanctions.[23]



[21] Benjamin Hilgenstock, Oleksii Hrybanovskii and Anatoliy Kravtsev, "Assessing Russia's Shadow Fleet: Initial Build-Up, Links to the Global Shadow Fleet, and Future Prospects", KSE Institute, June 2024, https://kse.ua/wp-content/uploads/2024/06/Global-Shadow-Fleet-June-2024.pdf.

[22] Benjamin Hilgenstock, Anatoliy Kravtsev, Yuliia Pavytska and Anna Vlaysuk, "Creating 'Shadow-Free' Zones – Proposal for the Implementation of an Insurance Requirement to Address Key Environmental Risks, KSE Institute, October 2024, https://kse.ua/wp-content/uploads/2024/10/Shadow_free_zones_October_2024_final.pdf.

[23] Infographic produced by Microsoft Co-Pilot.

In July 2025, the EU sanctioned two small regional Chinese banks, Heihe Rural Commercial Bank Co. Ltd. and Heilongjiang Suifenhe Rural Commercial Bank Co. Ltd., for providing crypto asset services that support Russia's war effort. These entities are highly unlikely to be the only entities that perform this kind of transaction. Hence, by using ship-to-ship transfers, Russian-sourced oil can then reenter legitimate global shipping networks through vessels that can negate compliance with international sanctions regimes. In addition to selling the oil at a price above the sanctions cap, the oil can then be transported on vessels with access to Western insurance and payment services.

The Russian use of the shadow fleet has serious implications, mostly importantly as a means to generate monetary funds. According to the Centre for the Research for Research on Energy and Clean Air, shadow fleets helped Moscow make 80 billion euros in revenue in a single year, a figure loosely equivalent to one-third of Russia's total income from petrochemicals. [24] In addition to the financial impact, shadow fleet ships are uninsured, structurally unsound, and use circuitous routes. Such dangerous practices are compounded by the refusal to use AIS during travel. The inherent risk of collision or shipwreck is then very high, and oil spills from such a collision could cause catastrophic ecological damage. Adding to this danger is the deliberate military targeting of Russian shadow fleet ships by Ukraine.

[24] "EU imports of Russian fossil fuels in third year of invasion surpass financial aid sent to Ukraine", Centre for Research on Energy and Clean Air, 10 April 2025, https://energyandcleanair.org/publication/eu-imports-of-russian-fossil-fuels-in-third-year-of-invasion-surpass-financial-aid-sent-to-ukraine/.

Teapot Refineries: How Chinese Companies Fund Russia's Oil Industry

A key system that Russia has been able to exploit to avoid sanctions is Chinese 'teapot refineries'. A teapot refinery is a small and privately-owned refinery that is outside of China's state-owned oil refining system. The teapot refineries were set up by the Chinese government as a means of promoting market competition and raising revenue at the provincial level. [25] By setting up teapot refineries, China hoped to push for more market competition, and force state-owned enterprises to reform and be run more efficiently. [26] Around 150 teapot refineries exist in China, most of them in coastal provinces like Shandong. [27] Since 2015, teapot refineries have been able to import crude oil. [28]

The system of teapot refineries is key to Russia's strategy of evading sanctions. Russian crude oil is loaded at Russian ports (for example Ust-Luga, Primorsk, and Novorossiysk) using the shadow fleet. [29] Some of these ships then sail directly to Chinese ports, and some conduct ship-to-ship transfers. Because these take place in international waters, moving the oil from a Russian carrier to another vessel before heading to China or India, makes the origin tracking process much harder. [30] Another important feature of teapot refineries is their independence from state firms, and as such, any purchases they make cannot be automatically attributed to the Chinese state. Thus, teapot refineries provide Beijing with a layer of plausible deniability. The refineries also have weak disclosure and reporting regimes, making tracking and monitoring their financial activities difficult. Teapot refineries are more willing to take risks handling Russian oil as they have no upstream interests in the West, are less diplomatically visible, and are accustomed to working in regulatory grey zones.

The importance of teapot refineries to generate money for Russia is critical, absorbing large volumes of oil that are no longer available for sale to Western countries. Furthermore, as noted, teapot refineries use shadow fleet ships, shell companies, and opaque payment systems to supply Russia with non-dollar currencies, reducing exposure to the reporting and surveillance of Western financial systems. Russia's export sales to teapot refineries help maintain the stability of Russian export volumes to fund the war effort. Indeed, Russia would struggle to maintain its war in Ukraine without the support of Chinese customers. [31]

[25] Joseph Webster, "Chinese refining markets 101 – and their implications for price caps on Russian oil", Atlantic Council, 8 March 2023, www.atlanticcouncil.org/blogs/energysource/chinese-refining-markets-101-and-their-implications-for-price-caps-on-russian-oil/.

[26] Erica Downs, "The Rise of China's Independent Refineries", Center on Global Energy Policy, 7 September 2017, www.energypolicy.columbia.edu/publications/rise-chinas-independent-refineries/.

[27] "I'm a (Not So) Little Teapot – The Surprising Influence of China's Independent Refineries", RBN Energy, 25 July 2017, www.rbnenergy.com/daily-posts/blog/surprising-influence-chinas-independent-refineries.

[28] "China's Private Oil Companies Struggle Against SOEs With New Tax Policy From Beijing", *Forbes*, 12 June 2018, www.forbes.com/sites/augustrick/2018/06/12/chinas-private-oil-companies-struggle-against-soes-with-new-tax-policy-from-beijing/.

[29] "Russia's Shadow Fleet: A Maritime Network to Evade Sanctions, its Operations, Destinations, and Comparison with the Fleets of Iran and Venezuela", *Hermes Kalamos*, 12 August 2025, www.hermes-kalamos.eu/russias-shadow-fleet-a-maritime-network-to-evade-sanctions-its-operations-destinations-and-comparison-with-the-fleets-of-iran-and-venezuela/.

[30] Ibid.

[31] Professor George Breslauer, "Vladimir Putin, A Life", Lecture #3: Putin as President, 2000-2008: Internal Policy, Osher Lifelong Learning Institute, UC Berkeley, Spring 2024, www.olli.berkeley.edu/sites/default/files/course/documents/Putin.OLLI%202Final.Spring%202024.The%20Early%20Decades.pdf.

Alternative Banking Systems Compensate for Loss of SWIFT

Following the invasion of Ukraine, the European Union banned several major Russian banks from the SWIFT system of international payments.[32] SWIFT is best thought of as a the 'plumbing' of international finance, providing international financial institutions with trusted, standardised message formats. As a result, transaction instructions are standardised, and are completed quicker while simultaneously reducing costs and the risk of errors. SWIFT is also powerful for regulatory and legal compliance, including sanctions. One critical aspect of SWIFT is that it provides an internationally standardised auditable and machine-readable record of international payments, including details of the sender, recipient, and purpose of transaction. From a sanctions enforcement perspective this is critical. When a SWIFT message for payment is sent, the message is screened against sanctions lists, watchlists, and national-level embargoes. This allows banks to avoid facilitating illegal transactions.

While a bank can technically process payments that are non-SWIFT, the process is costly, can be flagged for referral to risk compliance departments and law enforcement, and raise questions as to why the bank stepped outside of the standard internationally standard system. Therefore, some banks do not process non-SWIFT payments as a matter of company policy. By blocking major Russian financial institutions from using SWIFT, these institutions were no longer able to initiate or receive international payment messages, complicating international currency conversions and cross-border settlements. The original goal of SWIFT was to reduce the friction generated by complex international financial transactions, thus barring Russia from SWIFT was intended to increase financial transaction friction costs. As a result, Russian companies face longer delays and higher costs to process financial transactions.

Hypothesis: Russia would see a decline in SWIFT following exclusion

To establish if the SWIFT exclusions were genuinely constraining Russia, temporal data on Russian SWIFT message numbers were compiled, from 2022 when major Russian banks were banned from the system, through to 2024 when the last comparable data were available. If Russia was constrained, then the number of transactions would decrease over time. The results are shown in Figure 4.

Figure 4 clearly shows a dramatic drop in SWIFT activity in Russia. The decrease between 2022 and 2023, at 65%, was just the first year of the ban. This decline continued in 2024, with number of messages dropping to 18 million, a 25% decline from 2023 and an 85% decrease from the 2022 figure. Clearly, the SWIFT restrictions placed a dramatic strain on Russian banking systems. Therefore, the SWIFT ban, far from being symbolic, placed genuine and measurable real-life constraints on Russia's economy and increased the costs of business transactions.

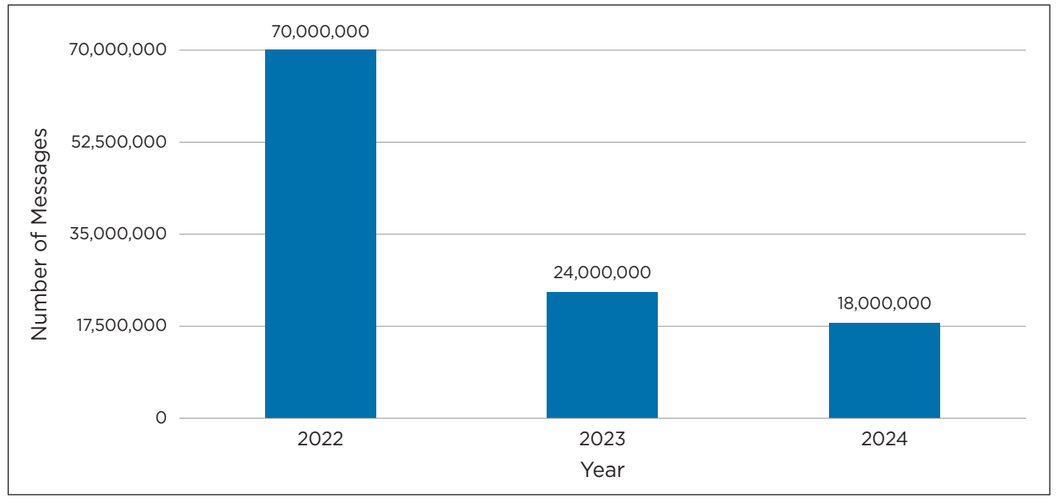
Adaptation

To counter the decline in SWIFT accessibility, Russia used its System for Transfer of Financial Messages (SPFS), originally devised in 2014 when Russia was threatened with being blocked from SWIFT due to the annexation of Crimea.[33] Since 2022, with the threat carried out, Russia has used SPFS. It is similar to SWIFT in that it is a financial messaging system, and like SWIFT, does not hold funds, or settle and clear transactions. However, compared to SWIFT, SPFS has the critical difference of being totally under Russia state control. Having established that the decrease in access to SWIFT had a measurable negative impact, SPFS can be similarly

[32] "Ukraine: EU agrees to exclude key Russian banks from SWIFT", European Commission, 2 March 2022, www.ec.europa.eu/commission/presscorner/detail/en/ip_22_1484.

[33] "Swift Sanctions Statement", Swift, 6 October 2014, www.swift.com/fr/node/16261.

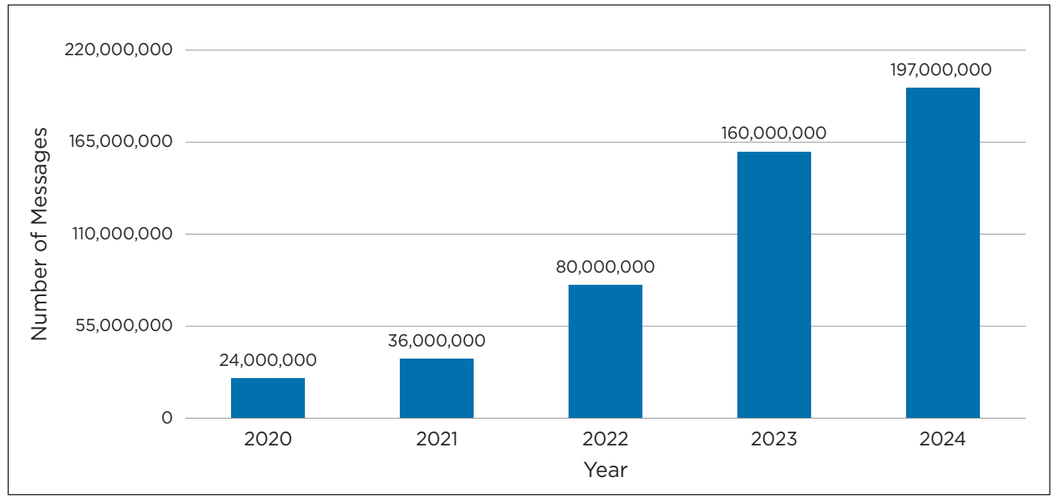
Figure 4: Number of SWIFT Messages by Russian Users (2022-2024).



Source: Foreign Intelligence Service of Ukraine (SZRU), 2025 report on Russian SWIFT activity.[34]

examined to see if, and to what extent, it was able to take the strain and replace the lost SWIFT traffic. To do this, data were analysed from multiple sources, as exact data across all years are not always publicly available. If the SPFS system represents an adaption strategy, then an increase in use would be expected over time – especially from the period when SWIFT became increasingly inaccessible to Russian entities and individuals. The results are shown in Figure 5:

Figure 5: SPFS Message Volumes for Russian Financial Institutions (2020–2024).



Sources: Bank of Russia, US Treasury, TASS state media reports; Bankinfobook. Where official absolute figures were unavailable (2021, 2022), values were derived from published percentage changes reported by the Bank of Russia and state media summaries.[35] All figures rounded to one decimal point.

[34] "Not a Single Russian Bank Has Been Able to Regain Access to SWIFT", Foreign Intelligence Service of Ukraine, 12 September 2025, https://www.szru.gov.ua/en/news-media/news/not-a-single-russian-bank-has-been-able-to-regain-access-to-swift.

[35] "Russia's SPFS to End SWIFT's Dominance", BankInfobook, 9 September 2025, https://www.bankinfobook.com/russias-spfs-to-end-of-swifts-dominance/; 20241121_spfs_alert.pdf; www.rbc.ru/newspaper/2022/02/28/621a68789a794737dade0c51; https://cyberft.com/about/comprasion/spfs.

Because the data were not always clearly stated, a degree of caution is therefore necessary. The method used to estimate message numbers was as follows. The Bank of Russia stated that there were 2 million monthly messages in 2020, therefore a yearly total of 24 million messages. [36] Although no absolute figure for 2021 was publicly available, the Bank of Russia states that the number of SPFS messages grew by 1.5 times in 2021, allowing for the figure of 36 million to be calculated. [37] The Bank of Russia stated that in 2023, 160 million messages were sent, a figure it said was twice the figure for the previous year. In 2024, the Bank of Russia's National Payment Systems Department estimated that the 2024 figure for SPFS messages had grown by 23% relative to 2023, therefore this provides a figure of 197 million messages. [38]

The SPFS system is not as reliable as SWIFT due to its smaller scale, inferior liquidity access, and limited international cooperation. [39] However, SPFS has allowed Russian banks to continue their domestic operations in the face of sanctions, so Russia has been able to better maintain domestic financial continuity than sanctions would have otherwise allowed in the absence of the SPFS system. In April 2024, Elvira Nabiullina, Director of the Central Bank of Russia, announced that 'nearly all' domestic Russian transactions were being conducted via the SPFS system. [40] In essence, Russia appears to have adapted and used its own system to sustain continuity under pressure from the West.

VISA, Mastercard, and Mir

In April 2022, Visa and Mastercard both announced they would no longer operate in Russia or with Russian merchants due to sanctions. These decisions were critical, because Visa and Mastercard are major international payment providers, connecting tens of millions of merchants and ATMs globally. Following its withdrawal, Russians could no longer use these payment systems for e-commerce, and their Visa and Mastercard cards linked to Russian banks would not work overseas. Foreign visitors to Russia were also no longer able to use their Visa or Mastercard to pay for goods or services with Russian providers. [41]

To outflank the Visa and Mastercard withdrawal ameliorate the potential impact, Russia began to activate an alternative it had been developing. In 2014, as Western sanctions over Crimea were imposed, Russia became aware of a critical financial vulnerability i.e., domestic payments that depended upon foreign payment service providers being prevented. To mitigate against this, Russia established the National Payment Card System of Russia (NSPK to use its Russian-language anacronym). The NSPK is a state-owned payment infrastructure operator, under the control of the Central Bank of Russia. [42] The system operates by routing all domestic payments by card, so the Russian government has immediate access to all data, and unlike in the West, does not require court orders to access it. Consequently, the NSPK system allows for maximum visibility for the Russian authorities, and critically, data does not leave Russia and become visible on Western systems such as Mastercard or Visa.

From the point of view of keeping transactions that may violate sanctions a secret from the West, NSPK is an ideal solution, given that its data are concealed from Western eyes. However, the primary purpose of NSPK was sanctions resilience rather than sanctions evasion.

[36] 2 million (messages) multiplied by 12 (months) = 24 million messages.

[37] 24 million multiplied by 1.5 = 36 million messages.

[38] Adding 23% to the 160 million figure gives a total of 197 million.

[39] "Bank of Russia's system for the transfer of financial messages (SPFS)", CyberFT, https://cyberft.com/about/comprasion/spfs.

[40] Luke Rodeheffer, "Russia Builds Alternative to SWIFT as Part of Digital Sovereignty Push", *Eurasia Daily Monitor*, Volume 21, Issue 67, Jamestown Institute, 5 January 2024, www.jamestown.org/russia-builds-alternative-to-swift-as-part-of-digital-sovereignty-push/.

[41] "Mastercard statement on suspension of Russian operations", Mastercard, 5 March 2022, www.mastercard.com/news/press/2022/march/mastercard-statement-on-suspension-of-russian-operations.

[42] " National Payment System", Bank of Russia, www.cbr.ru/eng/psystem/.

If payments were subject to being frozen by the West, then this could cause a collapse in the ATM system, generate bank runs, and increase financial panic that would threaten domestic order. The NSPK system meant that, at least in terms of domestic transactions, there was largely unbroken service continuity. For regime continuity and resilience, the provision of unbroken service was, and is, critical.

Within the NSPK network is the Mir payment system, and in Russian the word Mir has the double meaning of 'peace' and 'world'. Mir refers to both the network and to payment card system within it. Similar to other systems such as SPFS, its origins were in the 2014 period when Russia created backup systems to use in the event that Western sanctions were imposed. In 2018 Russian law mandated that all public sector employees receive their payments via the Mir system. [43] Russian law also requires pensions and other forms of welfare to be transferred solely to Mir accounts. [44] That specific legislation shows that Moscow had been planning a long-term and permanent opt-out from Western systems years before its invasion of Ukraine.

When Visa and Mastercard withdrew, the financial impact was less than expected as millions of Russians were already using a broadly equivalent payment system that was ready to be widely implemented. The most critical aspect of the Mir legislation and increased use was that it blunted the impact of Western sanctions, removed the leverage the West had, and allowed everyday economic life to continue relatively unaffected. While Mir lacks the international advantages of Visa and Mastercard, this is less important given the system's domestic focus. Mir worked as intended in reducing the impact of Western payment services withdrawing from the Russian market.

External Trade Adaptation, A7, and A7A5

The use of indigenous systems like NSPK and Mir have helped Russia take the strain of sanctions in terms of allowing continuity of domestic payments. While Mir is designed to solve the loss of SWIFT for internal Russian banking operations, A7 is used to solve issues with the loss of SWIFT for international transactions between Russia and third parties. A7 is not a single piece of technology, but rather multilayered parallel financial system. The A7 network is a critical system as it provides Russia with a pathway that Mir is lacking: a means to settle cross-border payments without the use of SWIFT, and with built-in methods to minimise scrutiny and traceability.

There are critical differences between a traditional promissory note and the A7 promissory note. A promissory note is standard credit instrument settled through regulated banks with traceability and enforcement. However, for an A7 promissory note, the credit is settled outside of SWIFT, using a combination of cash movements, cryptocurrencies, and networks of intermediaries in sympathetic or permissive jurisdictions. The A7 notes are explicitly designed to work outside the international banking system and therefore avoid the usual channels of reporting and monitoring that exist in the traditional international systems.

A7 is backed by the A7A5 stablecoin, a form of cryptocurrency traded on Tron and Ethereum blockchains. A7A5 is a Russian Ruble-backed token issued by the Kyrgyzstani company Old Vector, which was sanctioned by the US Treasury in 2025. [45] The cryptocurrency is banked by the (also sanctioned) Russian bank Promsvyazbank (PSB), which owns 49% of A7. [46] According to an analysis of trading patterns, A7A5 trades mostly take place between Monday and Friday,

[43] "Domestic scheme Mir disrupting Russian payment card market, says GlobalData", Global Data, 19 March 2022, www.globaldata.com/media/press-release/domestic-scheme-mir-disrupting-russian-payment-card-market-says-globaldata.

[44] Russian Federal Law № 88-ФЗ.

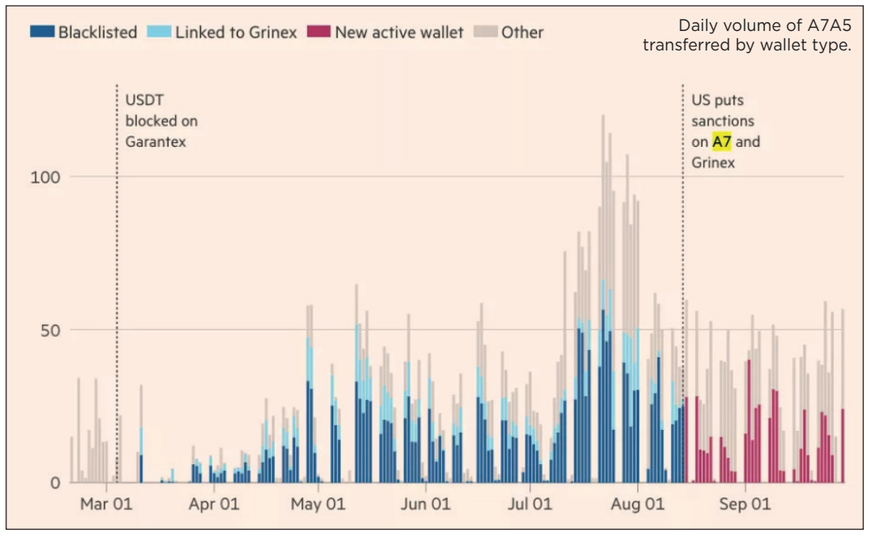
[45] "Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals", US Department of the Treasury, 14 August 2025, https://home.treasury.gov/news/press-releases/sb0225.

[46] "7A5: Circumventing Sanctions with Stablecoin Cryptocurrency", Centre for Information Resilience, www.info-res.org/app/uploads/2025/06/A7A5-Report-June-2025-Final-Draft-1.pdf.

suggesting it is used as a means of business transaction.[47] By the end of July 2025, A7A5 had processed an estimated $51.17 billion, and by mid-2026 the figure exceeded $100 billion.[48, 49] The majority of A7A5 trades are processed through DEX Grinex, the successor exchange to Garantex. The financial infrastructure of Garantex was disassembled in an international effort in March 2025, and two administrators were charged with money laundering by the US Department of Justice.[50]

Russia has facilitated the use of A7A5 by legalising crypto mining and cross-border crypto payments, reinforcing their role as tools to mitigate the impact of Western financial sanctions.[51] The A7 system can destroy and remint tokens as a means of breaking sanctions tracking links. By deleting old tokens linked to suspicious wallets and creating new tokens in fresh wallets, traceability is greatly reduced.[52] Although US authorities have used targeted sanctions against wallets linked to A7, its ability to remint tokens and switch quickly to new wallets undermines such restrictions. Around $86 billion worth of transactions have passed through the A7 network, including promissory notes, off-chain settlements, and non-A7A5 rails.[53] A7A5 has moved over $6 billion in crypto despite sanctions.[54]

Figure 6: The Reminting of A7A5 to Evade Sanctions.[55]



Source: *Financial Times* in *TradingView*

[47] "Legislated Sanctions Evasion: How the Garantex Rebrand, Grinex, and the Ruble-Backed Token, A7A5 Have Shaped Russia's Shadow Crypto Economy", *Chainalysis*, 14 August 2025, www.chainalysis.com/blog/a7a5-grinex-russian-crypto-economy-ofac-sanctions-august-2025/.

[48] Ibid.

[49] "Russia-Linked Stablecoin's Transactions Top $100 Billion in Year", *Bloomberg*, 22 January 2026, www.bloomberg.com/news/articles/2026-01-22/russia-tied-stablecoin-a7a5-tops-100-billion-in-transactions-despite-sanctions.

[50] "Garantex Cryptocurrency Exchange Disrupted in International Operation", Office of Public Affairs, US Department of Justice, 7 March 2025, www.justice.gov/opa/pr/garantex-cryptocurrency-exchange-disrupted-international-operation.

[51] "Legislated Sanctions Evasion: How the Garantex Rebrand, Grinex, and the Ruble-Backed Token, A7A5 Have Shaped Russia's Shadow Crypto Economy", *Chainalysis*, 14 August 2025, www.chainalysis.com/blog/a7a5-grinex-russian-crypto-economy-ofac-sanctions-august-2025/.

[52] "Russia-backed A7A5 stablecoin moved over $6B despite US sanctions: report", *Crypto.News*, 6 October 2025, www.crypto.news/russia-backed-a7a5-stablecoin-moved-over-6b-despite-us-sanctions-report/.

[53] "Sanctioned Russian crypto network sees $6 billion in cross-border payments", *Cryptopolitan*, 6 October 2025, www.cryptopolitan.com/sanctioned-russian-crypto-network-6-billion/.

[54] Ibid.

[55] "Russian ruble stablecoin A7A5 tied to Garantex successor: Financial Times", *TradingView*, 25 June 2025, www.tradingview.com/news/cointelegraph:71a6cb23e094b:0-russian-ruble-stablecoin-a7a5-tied-to-garantex-successor-ft/.

The Financial Times chart reproduced in Figure 6 shows how over 80% of the global supply of A7A5 was destroyed and then reissued following announcements of US sanctions. This was achieved by setting the wallet balances to zero – exploiting a smart contract function known as 'destroyBlackFund' – then tokens were placed in new active wallets, with the tokens given the name 'dirtyShares'.[56]

The use of cryptocurrency poses significant challenges for sanctions monitoring. As cryptocurrency analysts Chainalysis noted,

The emergence of the A7A5 network sanctioned today further illustrates how Russia is operationalising these alternative payment rails…Backed by sanctioned Russian institutions, A7A5 is providing a new, crypto-native avenue to bypass the ever-tightening sanctions against Russia.[57]

Russia's embrace of cryptocurrency underlines a key challenge in traditional sanctions monitoring and enforcement. As the digital and cryptocurrency pathways to commerce mature and deepen, the West's ability to pressure Russia will diminish. By using cryptocurrency, Russia can maintain financial flows that maintain state functioning, support the war in Ukraine, and increase the chances of regime survival.

[56] "Russia-backed A7A5 stablecoin moved over $6B despite US sanctions: report", *Crypto.News*, 6 October 2025, www.crypto.news/russia-backed-a7a5-stablecoin-moved-over-6b-despite-us-sanctions-report/.

[57] "Legislated Sanctions Evasion: How the Garantex Rebrand, Grinex, and the Ruble-Backed Token, A7A5 Have Shaped Russia's Shadow Crypto Economy", *Chainalysis*, 14 August 2025, www.chainalysis.com/blog/a7a5-grinex-russian-crypto-economy-ofac-sanctions-august-2025/.

Digital and Technical Communication Alternatives

It is not only alternative payment systems and financial workarounds that Russia regards as important in reducing the coercive power of sanctions. To counter Western control over, and pressure through information channels, Russia has built its own self-protective system of survival under constraint via its own social media platforms. In this sense, platform sovereignty aims to reduce the effect of narrative and information pressure exerted by Western platforms, similar to how Russian-controlled financial sovereignty seeks to reduce the effectiveness of sanctions. Western sanctions are frequently used to increase the likelihood of popular uprisings, and as such, any nation under sanctions increase population surveillance to ensure that uprisings are difficult to organise due to state disruption. Russia has a long-standing fear of popular uprisings and is especially motivated to prevent protests related to economic pain caused by war and sanctions.

Russian-controlled social media platforms work as a form of internet infrastructure, which enables adaptation. This adaptation is actualised by its ability to preserve the state's capacity to manage media narratives, mobilisation, and potential detection of anti-state messages and punishment of individuals. Comparable to how Russian financial systems provide reduced exposure to Western economic coercion, a Russian-controlled social media ecosystem reduces Western information and increases the narrative pressure. If Western-controlled platforms were allowed to operate in Russia, they would be a constant source of information that would contradict state-approved accounts of the war in Ukraine.

Economic sanctions have increased the pressure on the regime inside Russia. In such a climate, the need to impose greater internal coercion increases, and relies on both carrot (regime approved narratives to reduce social tension) and stick (the ability to monitor and then punish those pushing counter narratives). Notably, the regime's control does not directly coerce adversaries directly, rather it provides greater surveillance capacity used to support potential repression. As Andres Vosman of Estonia's Foreign Intelligence Service told reporters,

Every dictatorship is worried about losing control and therefore uses surveillance methods. We know that the Kremlin is very worried about how to mitigate potential tensions with likely radicalised or disappointed men returning from the war. [58]

In addition to monitoring for discontent or rebellion, state-controlled social media can help autocracies manage information warfare. Tighter state control of approved narratives via permitted platforms reduces the capacity for anti-regime mobilisation. The failure of autocracies in pre-Arab Spring countries to understand the power of Western social media platforms as a means to mobilise against the regime is a lesson Moscow learned well. [59] The Russian government carried out a study in 2020 to examine the potential implications for Russia of the Arab Spring's leverage of social media. [60]

Hypothesis: Russia would push Russian users away from western social media and into Russian-controlled alternatives

A credible hypothesis to test is that if Russia was using closer control of the internet, especially that afforded by Russian-native apps to maintain control, we would expect to see two things.

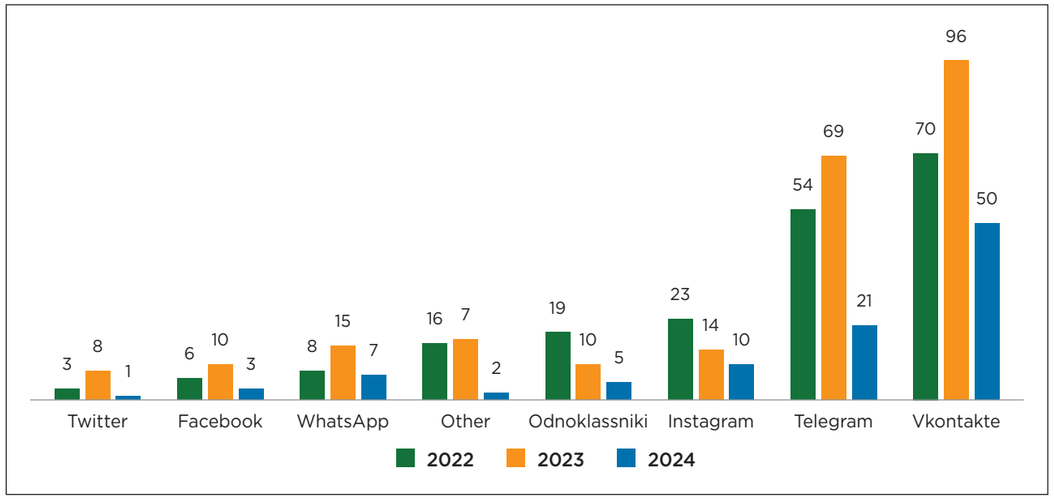
[58] "We Know that the Kremlin is Very Worried", *VSquare*, 20 January 2026, www.vsquare.org/we-know-that-the-kremlin-is-very-worried-interview-with-estonian-foreign-intelligences-top-analyst-andres-vosman/.

[59] Adam Smidi and Saif Shahin, "Social Media and Social Mobilisation in the Middle East: A Survey of Research on the Arab Spring", *India Quarterly* 73(2), June 2017, pp.196-209, www.jstor.org/stable/48505308.

[60] Ruslan Shangaraev and Olga Timakova, "Arab Spring Revolutions and Digital Technologies: Implications for Russia", *Advances in Social Science, Education and Humanities Research*, Volume 489, 2020, www.researchgate.net/publication/348058094_Arab_Spring_Revolutions_and_Digital_Technologies_Implications_for_Russia/fulltext/5ff1554492851c13fee3064a/Arab-Spring-Revolutions-and-Digital-Technologies-Implications-for-Russia.pdf.

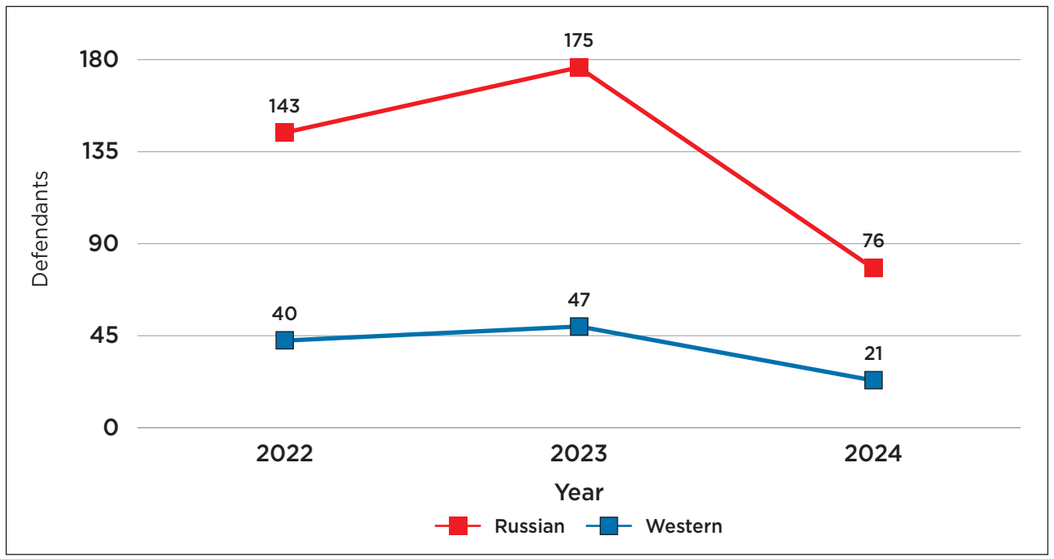
First, an increase in arrests for dissent, with most being for activities taking place on apps the Russian state has the closest supervisory control over. Second, we would expect to see a decline in dissent as the risks of being detected and punished increase as Russia's control of the internet tightened. To test this, data on social media-related arrests were compiled. The results are shown in Figure 7.

Figure 7: Number of Defendants in Social Media Post-Related Crime Cases (2022–2024). [61]



Source: OVD-Info. Chart by HJS.

Figure 8: Number of Defendants in Social Media Post-Related Crime Cases using Russian or Western Apps (2022–2024). [62]



Source: OVD-Info. Chart by HJS.

[61] "Persecution of the anti-war movement report: Three Years into Russia's Full-Scale Invasion of Ukraine", *OVD-Info*, February 2025, https://ovd.info/en/antiwar_3_years#1.

[62] Ibid.

As can be seen in Figure 8, the number of defendants linked to Russian-controlled platforms is higher than their Western counterparts. This is because their platforms are deeply integrated into Russia's domestic surveillance systems and as such, users are monitored closely. Although Western platforms were initially allowed to operate in Russia, they were less well integrated into Russia's surveillance architecture, with the Kremlin preferring restricting these tools to discourage uptake and push users towards Russian alternatives. This was an efficient tactic because it simply denied access to the platform rather spending the resources to monitor it. As predicted, a clear increase in arrests for dissent was present, especially for Russian-controlled apps. Online dissent then dropped as the state became better able to detect and punish opposition, discouraging further expressions of disagreement with official narratives.

In the case of Western social media platforms, outright bans led to both reduced opportunities for the expression of dissent and a reduced need for Russia to monitor the platforms.[63] Across both Russian and Western-controlled platforms, the reduction in defendants being prosecuted has decreased as the war continues, underscoring the effectiveness of online control and surveillance by Russian security forces, and the increased fear of expressing dissent given the increased control and risks. By restricting and banning Western platforms and pushing users towards closely surveyed Russian equivalents, Russia has successfully detected, punished, and reduced dissent. By doing so, Russia has enhanced regime survival against popular dissent at a time of constraint caused by war and economic privations.

63 "Analysis: Russia's 2024 digital crackdown reshapes social media landscape", *BBC Monitoring*, 17 February 2025, https://monitoring.bbc.co.uk/product/b0003arz.

Russia and the Sovereign Internet

The global economic system is underpinned and facilitated by a free and open internet. Although such a system is critical to globalisation and an international economic order, it is a potential threat to autocrats - partly due to it exposing their citizenry to ideas that challenge elite power and approved narratives, and partly because much of the architecture of the internet is dominated by the West, especially the United States. At the heart of Western internet architecture and governance are several principles and features. These features include multi-stakeholder management, a legal veil of separation between political authority and infrastructure management, and a general unspoken assumption that the internet is an open and interoperable space. A variety of bodies such as the Internet Corporation for Assigned Names and Numbers, and the Internet Engineering Task Force all operate alongside enterprise and civil society to maintain this internationalised and open version of the internet.

Russia has always viewed the Western-dominated internet space with suspicion seeing it as a potential highway for political dissent. Russia has therefore always feared that its own commerce and online activities could be subject to Western control and 'kill switch' threats in the event of a deterioration in international relations. While relations between Russia and the West were relatively calm for much of Putin's premiership, they have been turbulent since the 2008 war in Georgia, the annexation of Crimea in 2014, and the invasion of Ukraine in 2022. Currently, international relations are at their lowest point, with Russia feeling it needs to wrestle its own internet away from Western control.

The desire to create digital autarky on the internet has been a long-term plan of the Kremlin. The primary reason is the belief the West is using the internationally controlled internet as a way to harm Russia. In 2014, Putin told an audience of media professionals in Saint Petersburg that '...the Internet emerged as a special project of the US CIA, and is developing in the same vein'.[64] This paranoia, stoked at the time by Western reactions to Russia's annexation of Crimea, lays at the heart of the Putin regime's view of the internet. It is not seen as a politically neutral highway for commerce and exchange of ideas, but as a political project of the US security forces to penetrate and subvert rival nations. This tendency to view everything through a threat lens is common in Russian government circles.

To overcome perceived Western control, Russia has rapidly developed what it calls the 'sovereign internet'. According to OVD-Info, an organisation that monitors internal Russian repression, three legal instruments formed the backbone of the Russian sovereign internet: the Information Security Doctrine, the Strategy for Countering Extremism, and the National Security Strategy of Russia. In each case, a national security motive was invoked for greater state supervision over international internet traffic. Threats to national security were often, and conveniently, vaguely defined – giving the authorities maximum authority to act.

Foreign internet service providers in Russia, including giants like Google, Facebook, and Twitter, were a source of concern to Russian authorities. In 2021, the Russian parliament (Duma) passed a law intended to more tightly control these social media giants. The law obligated these firms to open representative offices on Russian territory and then to hold the firms to account for refusing to comply with Russian limits to access certain materials. The firms were subjected to an increasing number of calls to restrict or remove content from their platforms and repeatedly fined for violations.

64 "Internet blocks as a tool of political censorship", *OVD-Info*, 7 June 2022, www.ovd.info/en/internet-blocks-tool-political-censorship.

Overseeing the ‘sovereign internet’ is the Russian state communications regulator Roskomnadzor. This agency is central to Russia’s control of the internet, even more so since 2024. To limit Russian citizens’ access to information, Roskomnadzor makes heavy use of Technical Means to Counter Threats (TSPU to use the Russian-language anacronym). TSPU works in a similar fashion to a firewall, but unlike traditional firewalls – which simply block access to certain ISPs – TSPU identifies specific pieces of information within encrypted internet traffic. Then, via means of deep-packet inspection routines, it can rate-limit traffic and access, rather than completely preventing access. By rate-limiting traffic, pages load slowly, graphics and photographs load very slowly, and users often give up trying to access the information. This technique of slowing or ‘throttling’ traffic is recognised by researchers as an emerging censorship technique. [65]

When Russia invaded Ukraine in 2022, the Kremlin drastically increased its censorship powers. In March 2022, Facebook’s parent company Meta was declared an ‘extremist organisation’. Further, Facebook was banned on the grounds it discriminated against Russian state media (for example Russia Today and Sputnik) and was being used by foreigners to call for attacks on Russian troops in Ukraine. Although initially WhatsApp, also owned by Meta, was allowed to continue operating as it is a messaging app and not a content distribution platform, Russia has since banned it. The Duma’s Deputy Head of the Committee on Information Policy stated that WhatsApp should ‘prepare to leave the Russian market’. [66]

[65] Diwen Xue, Reethika Ramesh, Valdik S. S., Leonid Evdokimov, Andrey Viktorov, Arham Jain, Eric Wustrow, Simone Basso and Roya Ensafi, “Throttling Twitter: An emerging censorship technique in Russia”, in Proceedings of the 21st ACM Internet Measurement Conference (IMC ’21) (pp.435–443), Association for Computing Machinery, 2 November 2021, https://doi.org/10.1145/3487552.3487858, https://dl.acm.org/doi/10.1145/3487552.3487858.

[66] Andrei Soldatov and Irina Borogan, “Browser History: The Kremlin’s Newest Weapon”, Center for European Policy Analysis, 30 July 2025, www.cepa.org/article/browser-history-the-kremlins-newest-weapon/.

Pushing Users into Russian Internet Alternatives

Russia has been broadly successful in creating alternatives to Western-controlled banking networks and systems. These systems, coupled with cryptocurrency, shadow fleets, and the compliance of third countries, have helped Russia to bear the strain caused by Western sanctions. In addition to its own state-controlled banking and payment systems, Russia has been keen to promote domestic alternatives to Western social media. By doing so, Russia substitutes popular but now inaccessible Western social media for its own equivalents, reducing popular resentment. A domestic social media ecosystem also allows the Kremlin to insulate its people from outside information and more closely monitor their activities online.

One of the main motives for banning or throttling Western internet platforms is not just to shield Russian users from foreign information. Another reason is to essentially nudge Russian users away from Western-owned platforms and onto domestic alternatives. Such alternatives are ultimately under the control of the Russian security forces. Particularly younger Russians, who have grown up as ‘digital natives’, have enjoyed free contact with Western users, and are unhappy about such constraints. They present a potentially subversive strata of the population from the point of view of the Putin regime. As such, substitute platforms are needed to replace those lost due to sanctions.

Max

Among the most significant developments in Russia since the invasion of Ukraine has been the introduction of the app ‘Max’. The app was developed in 2024 by VK, the same Russian company that developed the Russian-language social media app VKontakt. [67] The Max app is very different from apps in the West, and represents one of the most significant attempts by Moscow to centralise control over the internet and achieve device-level control and monitoring of citizens. [68] Unlike traditional apps, which generally serve only one purpose (e.g. sending messages and paying bills), Max is an all-in-one app that facilitates multiple operations: such as paying bills, presenting digital ID, and accessing government services. The app has been mandatory on all new cell phones in Russia since September 2025, and frequently comes pre-installed. [69] Max is deeply linked to the Russian state and its desire to centralise (and thus more easily monitor) the daily activities of its citizens. Crucially, the app designers have close links to the Kremlin, meaning that unlike Western apps, which have the ecosystem of a private company, Max is deeply integrated with the Kremlin. Additionally, Western apps, which have been banned or throttled, and must compete commercially, Max enjoys the full financial backing of the Russian government. [70]

Max plays a key role in Russia’s adaptation to post-invasion sanctions. The app is a powerful tool in the development of the Russian ‘splinternet’. It provides a parallel internet architecture that allows the Kremlin to achieve two objectives. First, it allows Russia to strengthen domestic control, which in a time of war, is particularly important. Second, it allows Russia to nudge Russian users away from the Western-dominated internet, isolating them from Western

[67] “Putin Has a New Tool to Monitor Russians”, *The Atlantic*, 11 October 2025, www.theatlantic.com/international/archive/2025/10/russia-super-app-max/684524/.

[68] “Briefing – The MAX App: Russia’s Pocket-Sized Approach to Mass Surveillance”, Commission on Security and Cooperation in Europe, US Helsinki Commission, 2 December 2025, www.csce.gov/press-releases/briefing-the-max-app-russias-pocket-sized-approach-to-mass-surveillance/.

[69] “Russia orders state-backed Max messaging app preinstalled on all devices”, *TechSpot*, 21 August 2025, www.techspot.com/news/109158-russia-orders-state-backed-max-messaging-app-preinstalled.html.

[70] “The MAX App: Russia’s Pocket-Sized Approach to Mass Surveillace”, Joint House and Senate Hearing, 119th Congress, 2 December 2025, www.congress.gov/event/119th-congress/joint-event/LC75090/text.

influence, and compensating Russian users for the lost access to previously popular Western apps and services.

Yappy

The Yappy app is a platform for short form videos – 'shorts' – modelled closely on TikTok in terms of how function. While Russia is aligned with China, TikTok was still seen as being under foreign control and therefore less subject to total Russian state management and control as the Kremlin would wish. [71] The Yappy app was developed by Gazprom Media, which is part of the state oil company. [72] Yappy was launched in November 2021, and by the end of the year had one million downloads and 700,000 active users. [73] However, following the invasion of Ukraine and restrictions on access to Western social media, Yappy's user numbers increased substantially. By May 2022, Yappy's monthly active users were over 3 million. [74] By the end of 2022, its active audience had reached 8 million people. [75] The last reliable statistics on user numbers showed that 11 million people were using the app. [76] By promoting the use of Yappy, Russia further strengthened its native and state-controlled social media ecosystem, deepening the splinternet between Russia and the outside world. Furthermore, Yappy, like all domestic equivalents to Western social media, allows the Kremlin to closely control and monitor content.

RuRube

Like Yappy, RuTube is owned by Gazprom Media, underlining Russian state control over social media. RuTube was set up in 2006 as a Russian version of YouTube. In the aftermath of the invasion of Ukraine in 2022, it acted as a replacement for the Google-owned video sharing platform YouTube, which had been subject to throttling and demonetisation following the invasion of Ukraine. To offset these developments, the Kremlin again steered Russian internet users away from Western social media towards domestic, state-controlled alternatives. RuTube's user numbers jumped from 7.7 million users in January 2022 to over 50 million just three months later. [77]

71 "Russia launches 'Yappy', its homemade Tiktok", *Economic Times (India)*, 12 December 2021, www.brandequity.economictimes.indiatimes.com/news/digital/russia-on-verge-of-throwing-out-chinese-tiktok-launches-yappy-its-homemade-tiktok/88234030.

72 "Gazprom Media", State Media Monitor, 16 August 2025, www.statemediamonitor.com/2025/08/gazprom-media/.

73 "Yappy app has been downloaded more than 1 million times", *Gazprom Media*, 27 December 2021, https://www.gazprom-media.com/ru/media/prilozhenie-yappy-skachali-bolee-1-milliona-raz.

74 "Yappy's audience has reached 3 million people", *Gazprom Media*, 13 May 2022, https://www.gazprom-media.com/ru/media/auditoriya-yappy-dostigla-3-mln-chelovek.

75 "Gazprom-Media Holding announces the results of the first year of operation of YAPPY", *Gazprom Media*, 1 December 2022, https://www.gazprom-media.com/en/media/gazprom-media-holding-soobshchaet-ob-itogah-pervogo-goda-raboty-yappy.

76 "The monthly audience of the Russian video platform Yappy has crossed the threshold of 11 million users", *TASS*, 17 June 2023, http://www.tass.ru/ekonomika/18045761.

77 "Rutube traffic grew by 490% in March, reaching 50.1 million visits", *Kanobu*, 7 April 2022, www.kanobu.ru/news/trafik-rutube-v-marte-vyiros-na-490-i-dostig-501-mln-poseschenij-450483/.

The Cost and Threat to the UK

Although there has been a concerted effort by NATO countries and their allies to impose sanctions on Russia, the UK has borne a particularly heavy load in terms of sanctions enforcement. UK agencies and regulators such as the Office of Financial Sanctions Implementation, Office of Trade Sanctions Implementation, and the Financial Conduct Authority have worked hard to enforce sanctions, with obvious cost and time implications to the UK taxpayer. Over £25 billion in Russian assets were frozen in the UK because of war sanctions. [78] UK–Russia trade dropped drastically, with a 98% reduction in imports and a 77% reduction in exports. [79] The UK is a major centre for maritime insurance. The London market for maritime insurance contributes £49 billion to the UK economy. [80] Russia's shadow fleet activity has increased costs to UK maritime insurers due to lengthier and more complex diligence-compliance checks. These checks are important to prevent insurers from unwittingly insuring a vessel that is subject to sanctions, high-risk of accident, or both. [81] Such risks are increased by the shadow fleet operators' tendency to use false flags, changed names, and complex company registration tactics to obscure true ownership. [82] Furthermore, shadow fleet vessels often operate with no liability coverage or with fraudulent insurance paperwork, forcing more time consuming manual verification checks on the part of legitimate insurers. [83]

The cost and risks of challenging shadow fleet ships in UK territorial waters are a real issue due to Russian attempts to evade sanctions. The UK's Department for Transport confirmed that as of mid-2025, they had challenged 343 ships in its territorial waters on suspicion of being part of the Russian shadow fleet. [84] While no statistics were provided regrading what percentage of these ships were able to provide genuine ownership details, "several ships" were unable to provide documentation. One example cited by the Department for Transport was the Gambia-flagged tanker *Ailama*, which despite failing to produce satisfactory proof it was not part of the shadow fleet, continued to sail through the English Channel carrying crude oil loaded in the Russian port of Primorsk. [85] The risk of uninsured and/or structurally unsound vessels in the English Channel poses a tremendous ecological risk in the event of an oil spill, especially as it is one of the most congested maritime corridors in the world. Hence, the risk of a collision, especially considering the tendency of shadow fleet ships to turn off AIS navigation, is very high. [86]

The UK has prosecuted individuals based in Britain who attempted to help Russia evade sanctions. In April 2025, two individuals were found guilty of eight counts of breaching financial sanctions and two counts of money laundering. [87] This case was the first ever prosecution for

78 "UK sanctions freeze £25bn of Russian assets", HM Treasury, 21 March 2025, www.gov.uk/government/news/uk-sanctions-freeze-25bn-of-russian-assets.

79 "How UK Sanctions on Russia are Shaping the UK Economy", Linkilaw, 10 June 2025, www.linkilawsolicitors.com/insights/how-uk-sanctions-on-russia-are-shaping-the-uk-economy/.

80 "The London Market remains a significant contributor to the UK economy, but regulatory support is key to maintaining primacy", *London Matters*, May 2024, www.lmg.london/wp-content/uploads/2024/05/London-Matters-2024-Data-Pack.pdf.

81 "Sanctions & Shadow Fleet in 2026: The Compliance Playbook to Avoid Losses, Detentions and Banking Rejections", *Maritime Nexus*, 30 January 2026, www.maritimenexus.com/insights/sanctions-shadow-fleet-2026.

82 "More sanctions, more risk for carriers", *Insurance Business*, 22 September 2025, www.insurancebusinessmag.com/us/news/breaking-news/more-sanctions-more-risk-for-carriers-550433.aspx.

83 Ibid.

84 "More than 90% of shadow fleet ships are producing insurance certificates when challenged", Lloyd's List, 11 July 2025, www.lloydslist.com/LL1154189/More-than-90-of-shadow-fleet-ships-are-producing-insurance-certificates-when-challenged.

85 Ibid.

86 "Shadow Fleet Collisions: Meaning, Risks & Insurance Impact", FDR, www.fdr-risk.com/shadow-fleet/.

87 "Sentencing: The first ever UK prosecution of Russian sanction breaches", The Crown Prosecution Service, 11 April 2025, www.cps.gov.uk/cps/news/sentencing-first-ever-uk-prosecution-russian-sanction-breaches.

breaking Russian sanctions in the UK. In addition to prosecuting UK-based individuals, the UK has sanctioned foreign nationals for attempting to facilitate Russian evasion of UK sanctions.[88]

[88] "UK targets sanctions circumvention and crypto networks exploited by Russia", Foreign, Commonwealth and Development Office, 20 August 2025, www.gov.uk/government/news/uk-targets-sanctions-circumvention-and-crypto-networks-exploited-by-russia.

Conclusion

The Russian invasion of Ukraine triggered justifiable and far-reaching sanctions across a range of communication and commerce channels. At first, the sanctions appeared to punish Russia; but in the years that followed, Russia shows little sign of being economically weakened. Moscow has built alternative platforms that substitute their Western equivalents with new or near-new platforms that are beyond Western control. These platforms also function as a means of centralising and increasing monitoring of economic activity, helping the Kremlin to better control its population. When Russia has been unable to build domestic substitute systems or platforms, it uses methods ranging from shadow fleets to cryptocurrency abuse to illegally evade sanctions.

A key reason Moscow has been able to maintain its war in Ukraine is its ability to economically withstand Western financial pressure. The creation and maintenance of systems of commerce outside of Western control has been decisive in this endeavour. Other autocracies are noticing that motivated countries can build platforms outside of Western-controlled systems. Russia's allies have a shared interest in building systems outside of Western control and coercion. There are already signs that countries such as Belarus, Iran, and African nations in the 'coup belt' of the Sahel are considering such systems.

The West was confident that Russia's reliance on their systems would allow Moscow to be brought to heel relatively quickly. This belief was especially true given the apparent lack of alternatives to Western models, and Russia's depth of integration into the Western system pre-2022. However, Russia strategically adapted in response, and managed to do so at surprising speed. The adaptation was aided by scaling up pre-2022 assets and then fast-tracking new Russian-controlled substitutes for Western systems and platforms. These actions decoupled Russia from systems where the West could apply constraints and thus ameliorated the impacts of sanctions.

Where Russia could not create domestically controlled variants, it used extant systems of trade, payment, and communication via means that obfuscate the source. These included cryptocurrency and shadow fleets, often assisted by the anonymity of the activities and the fact trade partners within those systems were often sympathetic to Russia's anti-Western stance.

Policy Recommendations

- Encourage the adoption of blanket bans on engagement with Mir payment platforms, ensuring that secondary sanctions exist for banks that acquire Mir transactions or act as payment agents within that system.
- Pressure third countries tempted to facilitate Mir system payments to abandon the system and potentially encourage this abandonment by offering access to Western alternatives. Kyrgyzstan and Armenia were successfully lobbied by the West into not joining the Mir system, so there is precedent for this strategy. [89]
- Impose sanctions on all parts of the A7A5 system, including sanctions against cloud service providers, server farms, and data centres. Crypto exchanges must delist all tokens pegged to the Ruble, unless complete transparency is provided.
- Reposition sanctions efforts by shifting focus from entities to networks, and applying sanctions against networks rather than individual entities within them. This refocus would help to counter the tendency of Russian actors to use front companies or new companies. The US Treasury is applying sanctions on networks, showing this strategy can produce results. [90]
- Sanctions on shadow fleet ships should expand to target the entire supply chain of ships. Secondary sanctions should be applied to brokers or owners who are selling older ships into shadow fleets.
- Apply fast-track Port State Control inspections on ships presenting at ports which allows suspicious vessels possibly linked to the shadow fleet to be immediately inspected ahead of normal queues. These fast-track inspections could be coupled with environmental and safety concern detentions of poorly maintained vessels under ISM Code rules. Neither PSC nor ISM Code measures would require new sanctions so could be applied quickly.
- Developers should test censorship-resilient technologies and build censorship-resistant technology into products. Evading the Russian-controlled internet ecosystem is difficult but not impossible. These measures would avoid exposing Russian users to legal penalties, as would be the case with giving them VPN access.
- Expand diplomatic pressure on countries and companies that potentially provide support to Russia's censored internet. This pressure could include export bans, secondary sanctions, and transparency obligations on firms that sell technology or software that could be used for internet surveillance in Russia.

89 "Briefing: Russia puts on brave face as allies snub its Mir payment system", *BBC Monitoring*, 2 May 2024, https://monitoring.bbc.co.uk/product/b0001jc2.

90 "Treasury Sanctions Cryptocurrency Exchange and Network Enabling Sanctions Evasion and Cyber Criminals", US Department of the Treasury, 14 August 2025, http://www.home.treasury.gov/news/press-releases/sb0225.

Title: “WHY SANCTIONS ARE NOT WORKING: HOW RUSSIA IS ADAPTING AND SURVIVING”
By Michael McManus

The Henry Jackson Society
Millbank Tower, 21-24 Millbank
London SW1P 4QP, UK

www.henryjacksonsociety.org

HJS
Henry
Jackson
Society

DEMOCRACY | FREEDOM | HUMAN RIGHTS

CENTRE FOR RUSSIA AND EURASIA STUDIES

June 2026