FREE NETWORK POLICY BRIEF SERIES #AcademicsStandWithUkraine

Violaine D'Ortona, SITE and ENS de Lyon
Jonathan Lehne, SITE
Maiting Zhuang, SITE
June 2026

Towards a Russian Internet?

The internet enables information and opinions to flow rapidly and at low cost, including across national borders. It allows individuals to coordinate collective action on an unprecedented scale. Many authoritarian governments, therefore, seek to control the online information environment. This policy brief examines the evolution of internet control in Russia and documents how censorship and network disruptions have intensified since the full-scale invasion of Ukraine.

Drawing on three complementary datasets—Access Now's Shutdown Tracker Optimization Project (STOP), the Internet Outage Detection and Analysis (IODA) initiative, and the Open Observatory of Network Interference (OONI)—we document a sharp increase in internet disruptions, platform blocking, and website censorship in Russia since 2022. We argue that this expansion of censorship was enabled by a longer-term shift from a relatively decentralized system of internet regulation towards a centralised infrastructure capable of monitoring, filtering, and controlling internet traffic at scale.

The online war

The Russian government has been fighting its war against Ukraine on multiple fronts: aside from the battlefield in Ukraine, there is also an online front at home. Since the start of the full-scale invasion in February 2022, the Kremlin has sought to control how the war is presented to the Russian public. Within weeks of the invasion, Russia blocked Facebook, Instagram, and Twitter, and restricted access to numerous foreign and independent media outlets. In the years that followed, restrictions expanded to include VPN services and specific features of messaging platforms such as WhatsApp and Telegram.

These measures are not isolated events. Rather, they represent the latest stage in a broader effort to control the Russian internet. Over the past decade, Russia has gradually built the legal and technical infrastructure needed to monitor, filter, and disrupt online communications. The war in Ukraine has revealed the extent of these capabilities and accelerated their deployment.

This brief examines how internet control in Russia has evolved in recent years. We discuss the challenges of measuring internet censorship and analyse evidence from three complementary datasets. Together, these measures show a sharp increase in internet disruptions, platform restrictions, and censorship since the full-scale invasion of Ukraine.

Why control the internet?

The internet has transformed the way information is produced, shared, and consumed. It allows information and opinions to spread rapidly at low cost, including across national borders, and enables individuals to coordinate collective action on an unprecedented scale. For an authoritarian government, the internet allows the spread of information that contradicts official narratives and can facilitate political opposition. The role of social media in mobilising protests during the Arab Spring highlighted the power of the internet.

In response, many authoritarian governments have sought to exert greater control over the internet. China is the most advanced example of state control over the online information environment. Through its ``Great Firewall'', the Chinese government controls access to foreign information and platforms, while influencing and monitoring domestic online activity through censorship, regulation, and the cooperation of domestic technology companies.

Russia has historically taken a different approach. Until recently, Russians retained access to many Western platforms, and internet censorship was implemented in a relatively decentralized manner by internet service providers. Rather than constructing a separate internet from the outset, Russia sought to control information flows while remaining integrated with the global internet.

Authoritarian trade-offs

Why might the Russian government have followed this light-touch approach, and why change course now? The literature in economics and political science describes two trade-offs an authoritarian government faces when deciding how much control to exert over the internet.

The first is economic. Describing the 'dictator's dilemma,' Kedzie (1997) writes, "*it may now be*

virtually impossible for any country to maintain an open economy for expansion while remaining closed to democratic ideas". Estimates of the economic cost of internet shutdowns support this argument. One estimate suggests that government-imposed outages cost the global economy $19.7 billion in the year 2025 (Migliano 2026).

The second is informational. Egorov et al. (2009) argue that an authoritarian government that constrains free media and communication flows too aggressively cuts itself off from information required to govern effectively. Local bureaucrats have no incentive to perform in the absence of reliable independent monitoring. King et al. (2013) provide empirical evidence for this in the context of Chinese social media censorship. They find that censors allow (potentially informative) criticism of the government but specifically target posts that could give rise to collective action.

Controlling the narrative around a prolonged, costly war necessitates a greater level of intervention. The censorship strategies discussed below can be viewed through the lens of a government seeking new ways to navigate both trade-offs.

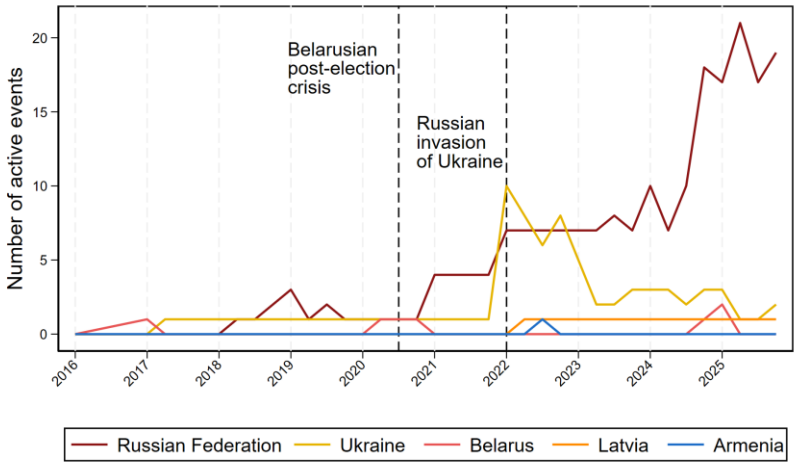
Tracking internet shutdowns

Identifying government-imposed internet shutdowns is challenging. Affected users will typically have no way of verifying the extent or true cause of an outage, and their ability to report it in real-time may itself be curtailed. As a result, organizations that monitor internet shutdowns use very different methodologies. In our brief, we will describe three of the most prominent publicly available datasets that attempt to track disruptions to internet services worldwide.

Access Now, a member of the #KeepItOn coalition, provides a publicly available dataset of internet shutdowns through its Shutdown Tracker Optimization Project (STOP). The distinguishing feature of STOP is that it establishes intent. It combines technical data on internet connectivity with either official government statements or information provided by informed insiders. STOP records various types of technical disruption: from full blackouts to throttling and partial service restrictions. However, a measured disruption of internet services is only recorded as a *shutdown event* if it can be traced back to deliberate government intervention with a high degree of confidence. The advantage of this approach is that one can be confident that each instance in the data reflects a deliberate government-induced shutdown. The limitation is that the dataset likely undercounts shutdowns in data-scarce or highly repressive environments where establishing intent is not always possible.

Figure 1 plots internet shutdowns in Russia, and for comparison, the FREE network member countries from 2016 to 2025. The chart is dominated by the sharp upward trend in Russia, starting in 2021, and accelerating after the full-scale invasion of Ukraine. There is also an increase in Ukraine after the invasion; which includes both Russian actions that disrupted connectivity and Ukrainian measures to block specific Russian platforms. Similarly, Latvia imposed nationwide blocks of two Russian platforms after the start of the invasion. The chart also shows the internet blackouts in Belarus amid widespread protests following the 2020 election.

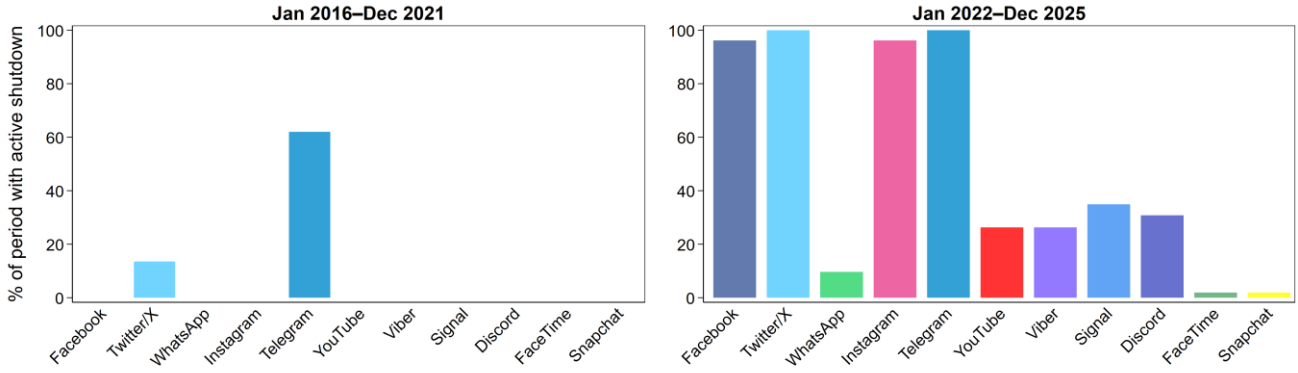
Figure 1. Internet shutdown events in FREE Network countries (2016-2025)



Source: Access Now, KeepItOn STOP (2016-2025) and authors' calculations.
Note: This chart shows the number of distinct intentional internet shutdown events active during each quarter in countries of the SIDA Free Network. (Sweden, Georgia, Moldova, and Poland are excluded from the graph because no shutdown events were recorded for them over this period.) An internet shutdown is defined as an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information (Access Now, KIO). A shutdown event can result from third-party interventions rather than be intended by the country's government.

Figure 2 uses the same dataset to illustrate which social media and online messaging platforms were most affected by the increase in government control of the internet in Russia. Relative to China, Russia used to exert only 'light-touch' control over the internet, as seen in the first panel of the figure. From 2016 to 2021, the social media and online messaging platforms in the chart were largely unaffected by shutdown events. The second panel shows that since early 2022, all of these platforms have experienced shutdown events, and in the case of Facebook, Twitter/X, and Instagram, there have been active blocks throughout the entire period.

Figure 2. Platform service disruptions in Russia (2016 – 2025)



Source: Access Now, KeepItOn STOP Dataset (2016-2025) and authors' calculations.

Note: This graph details the platforms affected by internet shutdowns in Russia (See Figure 1). Each bar shows the percentage of days in the period when at least one shutdown event affected the platform in Russia.

As discussed, the STOP dataset likely undercounts internet shutdowns. We therefore evaluate whether alternative measures show the same upward trend for Russia.

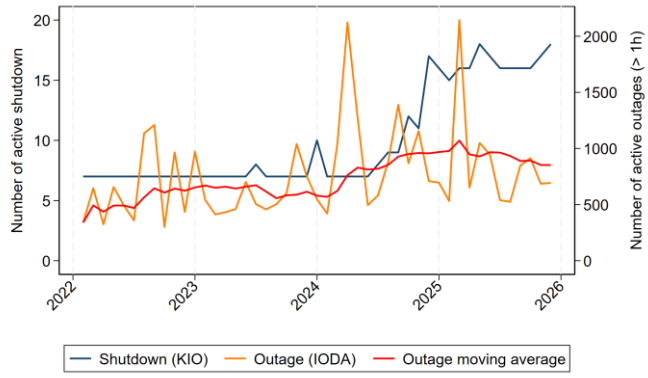
Our second dataset comes from the Internet Outage Detection and Analysis (IODA) initiative at Georgia Tech, which monitors global internet connectivity using three complementary technical signals to detect when networks go offline. IODA identifies outages at the country, regional, or network level and records their duration and severity. Importantly, unlike STOP, IODA detects outages but not their cause. An outage may reflect deliberate government action or infrastructure failure.

Panel (a) of Figure 3 compares the IODA measure of outages with the STOP measure of internet shutdowns for Russia. The IODA measure (right axis) is roughly 100 times as high as the STOP measure in any given period, as IODA records all detected disruptions regardless of intentionality. That said, the IODA data corroborate the finding that internet disruptions have become ever more frequent in Russia, with significant increases in 2024 and 2025.

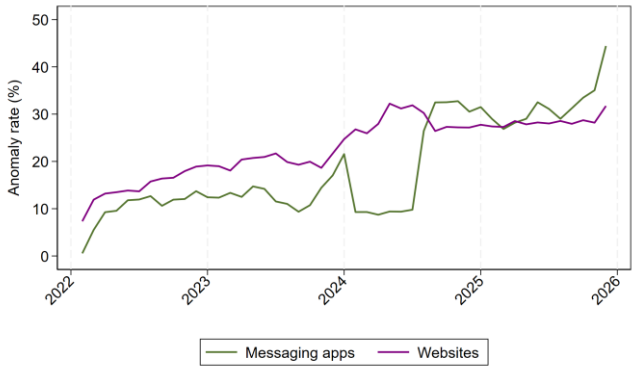
Our third dataset comes from the Open Observatory of Network Interference (OONI), which focuses on censorship rather than outages. OONI relies on volunteers running tests through an open-source app, generating measurements of whether specific websites, messaging platforms, and circumvention tools are accessible or blocked.

Figure 3. Trend in internet disruption and online censorship in Russia (2022-2025)

a. Count of internet disruptions



b. Rate of websites and apps censorship



Source: Access Now KeepItOn STOP (KIO), Internet Outage Detection and Analysis (IODA), Open Observatory of Network Interference (OONI), and authors' calculations.

Note: Panel (a) shows STOP internet shutdown events in the blue line, which records intentional disruptions of internet or electronic communication (KIO, see Figure 1), and IODA internet outages in the orange line, which are abnormal simultaneous drops in 2 or more signals measuring internet connectivity, intentional or accidental. IODA outages are filtered to only include events lasting more than 2 hours to match the KIO restriction. The red line shows a twelve-month moving average of IODA outages. Panel (b) shows online censorship rates for websites and messaging apps, measured by the monthly rate of anomalies recorded by OONI. An anomaly is detected when a measurement presents signs of potential network interference (such as the blocking of a website or app). Messaging apps data derive from OONI messaging platform availability tests (WhatsApp, Telegram, Signal, Facebook Messenger), and website data from OONI Web Connectivity tests on individual websites' availability. Days and platforms or websites with fewer than 5 measurements are excluded for reliability.

It does so by comparing results over the user's network against a control server, with divergences flagged as potential interference. The main limitation is uneven coverage over time, a consequence of the volunteer-based approach, though the total number of daily measurements is always known.

Panel (b) of Figure 3 plots anomaly rates for websites and messaging apps as experienced by Russian users since the start of 2022. Both lines show a clear upward trend, indicating that Russian users are increasingly encountering websites and apps that are blocked in Russia but available elsewhere.

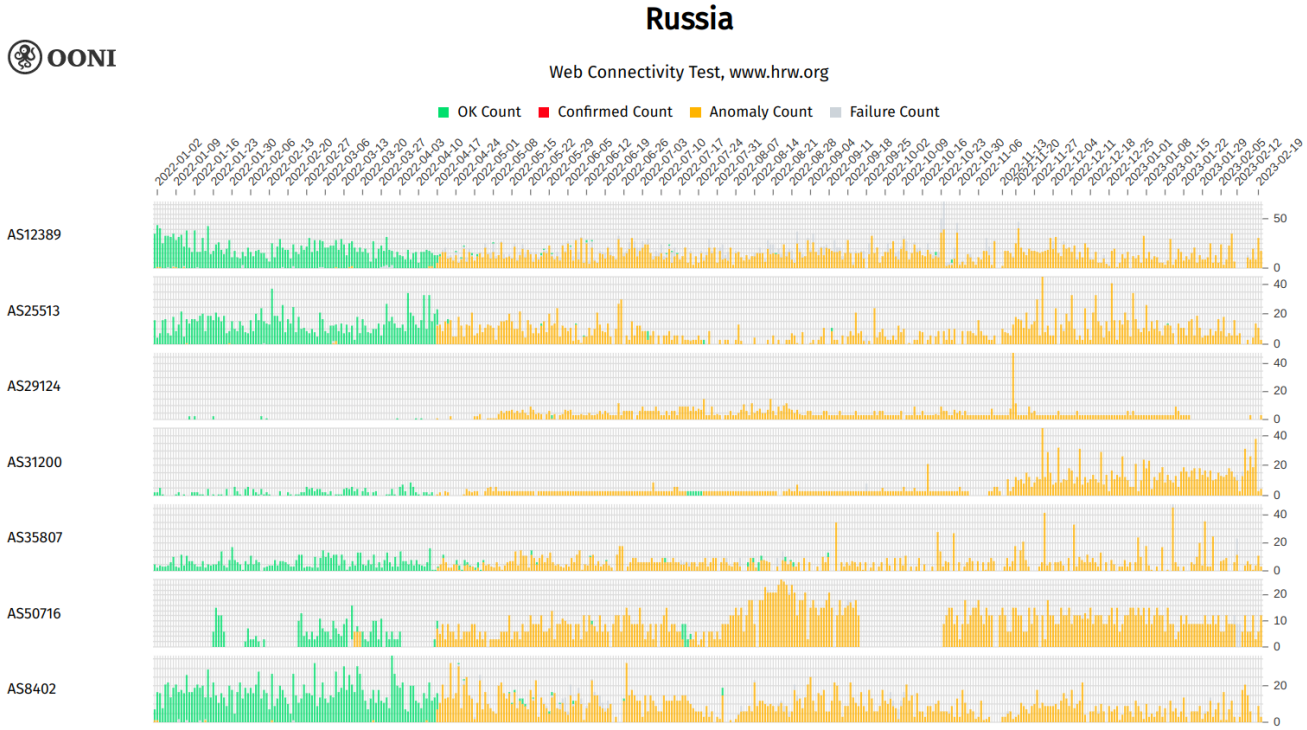
The centralisation of Russian internet control

While Russia has always exerted some degree of control over the internet, it has historically relied on what Ramesh et al. (2020) call a decentralised model. Since 2012, Russia's internet regulator, Roskomnadzor, has maintained a national blocklist of websites and required Internet Service Providers (ISPs) to restrict their users' access to these websites. As ISPs were granted full discretion over how to comply, the blocking mechanisms and their effectiveness reportedly varied significantly across websites and providers. The attempted blocking of Telegram in 2018 exposed the limitations of Russia's decentralized approach to internet censorship. To enforce the ban, Roskomnadzor blocked millions of IP addresses associated with Amazon and Google cloud services, leading to widespread disruption of unrelated online services, while failing to prevent Russian users from accessing Telegram.

Since then, Russia has moved towards a more centralised model of internet governance, aimed at increasing state control over its domestic internet and reducing dependence on the global network. In 2019, the "Sovereign Internet Law" (or "Law on Sustainable Runet") came into force, which provided the Russian state the legal and technical tools to centrally monitor, filter and reroute internet traffic. The law requires ISPs to install TSPU (Tekhnicheskie Sredstva Protivodeystviya Ugrozam, or "technical means of countering threats") devices on their networks, or face fines. These devices allow the government to track and manage internet traffic across private networks in a centralised manner (Human Rights Watch 2025).

TSPUs first attracted attention in 2021 when access to Twitter was throttled, but their impact has since become more widespread (Xue et al., 2021). In February 2023, OONI and the Russian digital rights organisation Roskomsvoboda reported that numerous media outlets and websites with critical coverage of the Russian war in Ukraine had been blocked in 2022. In a striking contrast to previous decentralised censorship practices, these restrictions were implemented simultaneously across internet providers. Figure 4, originally published by OONI, illustrates the simultaneous blocking of the Human Rights Watch website after it was added to Roskomnadzor's blocklist on April 17, 2022. The figure shows that users across multiple networks lost access at the same time. The OONI report also highlights that providers are now using the same technical methods to enforce central directives, illustrating the widespread effective use of TSPUs.

Figure 4: Network interference in Russia



Source: Open Observatory of Network Interference (OONI), Roskomsvoboda, How Internet censorship changed in Russia during the 1st year of military conflict in Ukraine.
Autonomous System Numbers (ASNs) which presented the largest volume of anomalies (more than 1,200 anomalies) in the testing of www.hrw.org in Russia between 1st January 2022 to 20th February 2023. An anomaly is detected when a measurement presents signs of potential network interference (such as the blocking of a website or app).

Recent restrictions on Telegram provide further evidence of their efficacy. In contrast to the failed block in 2018, most Russian users are now unable to access the app without VPNs or other workarounds.

The capabilities of TSPUs extend far beyond individual website blocking. Recent reports suggest that instead of just targeting specific parts of the internet, they are now used to impose temporary, near-total internet blackouts. These cut users off from much of the global internet, while preserving access to a whitelist of Russian government websites and fully cooperative platforms (Human Rights Watch, 2026). In doing so, TSPU moves Russia closer to the Chinese model of internet control, increasing the state's ability to manage internet traffic centrally.

Conclusion

In recent years, Russia's strategy towards internet censorship has changed profoundly. The decentralised, relatively light-touch approach, with unrestricted access to many Western platforms, has been abandoned. The government has acquired the legal and technical capability to exert tight, centralised control over service providers, and every indicator we have analysed in this brief makes clear that it is using these powers ever more aggressively.

The incremental nature of these changes and their technical sophistication mean that Russia's internet control cannot be equated with the blunt tool of country- or region-wide shutdowns as used by authoritarian governments in other parts of the world. These types of internet shutdowns are highly visible to domestic and international users and spark outrage. Russia's strategy is more insidious. Its citizens' access to the global internet has been shutting down, year by year and month by month. Individual users' experience of these changes is fragmented, making a collective response difficult. Russia is on its way to creating and controlling its very own version of the internet.

References

Access Now. 2026. "#KeepItOn Shutdown Tracker Optimization Project (STOP) Dataset." Accessed 15 Apr. 2026.

Access Now. 2026. "Shutdown Tracker Optimization Project (STOP): Tracking Internet Shutdowns — Our STOP Methodology."

Bischof, Zachary S., Kennedy Pitcher, Esteban Carisimo, Amanda Meng, Rafael Bezerra Nunes, Ramakrishna Padmanabhan, Margaret E. Roberts, Alex C. Snoeren, and Alberto Dainotti. 2023. "Destination Unreachable: Characterizing Internet Outages and Shutdowns." *Proceedings of the ACM SIGCOMM 2023 Conference*, 608–621.

Egorov, Georgy, Sergei Guriev, and Konstantin Sonin 2009. "Why resource-poor dictators allow freer media: A theory and evidence from panel data." *American political science Review* 103, no. 4: 645-668.

Human Rights Watch. 2026. "Russia: Internet Shutdowns Escalate." March 31.

Internet Outage Detection and Analysis (IODA). 2026. "IODA website."

Kedzie, Christopher R. 1997 "*Communication and Democracy: Coincident Revolutions and the Emergent Dictator's Dilemma.*" *RAND Document No: RGSD-127*.

King, Gary, Jennifer Pan, and Margaret E. Roberts 2013. "How censorship in China allows government criticism but silences collective expression." *American political science Review* 107, no. 2: 326-343.

Kruope, Anastasiia. 2025. "Disrupted, Throttled, and Blocked." Human Rights Watch, July 30.

Migliano, Simon 2026. "Cost of Internet Shutdowns in 2025" TOP10VPN Annual Internet Shutdown Report.

Open Observatory of Network Interference (OONI). 2026. "OONI Web Connectivity test."

Open Observatory of Network Interference (OONI). 2026. "OONI Website."

Ramesh, Reethika, Ram Sundara Raman, Apurva Virkud, Alexandra Dirksen, Armin Huremagic, David Fifield, Dirk Rodenburg, Rod Hynes, Doug Madory, and Roya Ensafi. 2023. "Network Responses to Russia's Invasion of Ukraine in 2022: A Cautionary Tale for Internet Freedom." *32nd USENIX Security Symposium (USENIX Security 23)*, August 2581–2598

Roskomsvoboda and OONI. 2023. "How Internet Censorship Changed in Russia during the 1st Year of Military Conflict in Ukraine." February 24.

Xue, Diwen, Benjamin Mixon-Baca, ValdikSS, et al. 2022. "TSPU: Russia's Decentralized Censorship System." *Proceedings of the 22nd ACM Internet Measurement Conference*, October 25, 179–94.

Xue, Diwen, Reethika Ramesh, Valdik S. S., et al. 2021. "Throttling Twitter: An Emerging Censorship Technique in Russia." *Proceedings of the 21st ACM Internet Measurement Conference*, November 2, 435–43.

Violaine D'Ortona

ENS de Lyon
Violaine.dortona@ens-lyon.fr
https://www.hhs.se/sv/persons/d/dortona-violaine/

Violaine is a master's student in the Advanced Economics program at the École Normale Supérieure (ENS) de Lyon, where she also completed her bachelor's degree. She is currently working as a research assistant at the Stockholm Institute of Transition Economics (SITE).

Violaine primary research interests lie in political economics, with a particular focus on its intersection with media.

Jonathan Lehne

Stockholm Institute of Transition Economics
jonathan.lehne@hhs.se
https://www.hhs.se/en/persons/l/lehnejonathan/

Jonathan is a Researcher at the Stockholm Institute of Transition Economics (SITE) – Stockholm School of Economics. He completed his PhD in Economics at the Paris School of Economics in 2020. He has previously worked as a research analyst at the European Bank for Reconstruction and Development. Jonathan's primary research interests are in political economy and development economics.

Maiting Zhuang

Stockholm Institute of Transition Economics
maiting.zhuang@hhs.se
https://www.hhs.se/en/persons/z/zhuangmaiting/

Maiting is a Researcher at the Stockholm Institute of Transition Economics (SITE) – Stockholm School of Economics. She completed her PhD in Economics at the Paris School of Economics in 2020. She has previously worked as an Economist at the Bank of England. Maiting's primary research interests are in political economy and development economics.

freepolicybriefs.org

The Forum for Research on Eastern Europe and Emerging Economies is a network of academic experts on economic issues in Eastern Europe and the former Soviet Union at BEROC (Vilnius), BICEPS (Riga), CenEA (Szczecin), ISET-PI (Tbilisi), KSE (Kyiv) and SITE (Stockholm). The weekly FREE Network Policy Brief Series provides research-based analyses of economic policy issues relevant to Eastern Europe and emerging markets. Opinions expressed in policy briefs and other publications are those of the authors; they do not necessarily reflect those of the FREE Network and its research institutes.

FREE NETWORK