BRIEFING PAPER
436
May 2026

Russia's new digital authoritarianism

Challenges and leverage for Europe

Margarita Zavadskaya

FIIA
FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

FIIA FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

BRIEFING PAPER 436 May 2026

Russia's new digital authoritarianism

Challenges and leverage for Europe

Summary

- Russia's 2025–2026 internet shutdowns and restrictions show that its digital authoritarianism has accelerated from content-level control, such as blocking individual websites, to controlling access at the network level.
- This approach poses a direct threat to Europe's normative and regulatory power by normalizing state control over the internet, undermining open-network principles, and promoting a sovereignty-first model of internet governance.
- Russia is not only tightening domestic control but also exporting censorship practices and technical capabilities, particularly to countries that cooperate closely with it. This helps spread authoritarian governance models beyond Russia's borders.
- Yet despite greater internal control, Russia's digital infrastructure is increasingly dependent on external supply chains, largely facilitated by China. This creates vulnerabilities that can be targeted through sanctions and export controls.
- The EU should treat the preservation of a rights-based, open internet as a core security objective. This involves countering the normalization of repression in global forums, enforcing restrictions on dual-use technologies, supporting resilient connectivity for civil society trapped in authoritarian states, and incorporating digital rights into its external partnerships.

Author

Margarita Zavadskaya
Senior Research Fellow
Russia, Eastern Europe and Eurasia
Finnish Institute of International Affairs

Introduction

Russia's internet environment is deteriorating visibly and sharply. Freedom House reports that internet freedom in Russia hit a new low in 2024–2025, coinciding with the government's intensified efforts to isolate users from the global network.[1] Systematic blocking, throttling, and shutdowns not only affect political activists and civil society groups, thereby tightening political control, but also disrupt banking, state services, and logistics. This demonstrates the broad collateral damage that can be caused by state intervention at the infrastructure layer.[2]

The current crackdown marks a structural shift: from controlling online content, such as by blocking certain websites and using whitelists, to governing the infrastructure that enables digital life. This is no longer episodic censorship but systems-level intervention, with the state using control over connectivity as part of wartime governance. Russia is moving towards a model in which internet access is managed at the network rather than the content level.

It is crucial to distinguish between internet shutdowns and service substitution. The current wave of restrictions is not intended to block the internet as a whole. Instead, it seeks to expand state-aligned digital platforms and tools that replace restricted global platforms: VK in place of X, Instagram, and Facebook; Max in place of Telegram; and Yandex in place of Google.

From the Kremlin's perspective, this shift serves multiple functions. It reinforces state control under wartime conditions and maintains political control over dissent. It also facilitates domestic mobilization to the front, while expanding the state's operational toolkit beyond its borders. In addition, it advances a sovereignty-first model of internet governance, in which state control over connectivity is prioritized over openness and global networks. However, this approach comes at a high cost, as efforts to maximize control undermine the very performance and reliability of Russia's digital infrastructure.

This Briefing Paper examines how Russia's emerging model of infrastructure-based digital authoritarianism is reshaping both domestic governance and the external security environment. It argues that the consolidation of centralized, scalable control over connectivity – enabled by the sovereign internet framework – strengthens regime resilience in the short term, while also generating systemic vulnerabilities and external dependencies that Europe can leverage.

The analysis proceeds in four steps. First, it conceptualizes Russia's shift towards infrastructure-level control as a staged transformation in digital authoritarianism. Second, it introduces the "control trap" mechanism and shows how intensifying control generates degradation, inefficiencies, and long-term governance risks. Third, it examines how the pursuit of digital sovereignty deepens Russia's dependence on external supply chains – particularly those involving China – and creates asymmetrical vulnerabilities. Fourth, it assesses how these dynamics intersect with Europe's exposure to critical infrastructure risks, cross-border spillovers, and competition over global internet governance norms.

1 Freedom House (2025) "Freedom on the Net 2025: Russia". Washington, DC: Freedom House. https://freedomhouse.org/country/russia/freedom-net/2025.

2 Litvinova, Dasha (2026) "Russia's internet crackdown leads to a spring of growing discontent". *The Hill*, 9 April. https://thehill.com/homenews/ap/ap-international/ap-russias-internet-crackdown-leads-to-a-spring-of-growing-discontent/.

The central argument is that Russia's digital-control architecture should not be understood solely as reinforcing regime strength. It is also a liability that creates leverage points for the EU across regulatory, economic, and security domains.

"Russia's digital-control architecture is also a liability that creates leverage points for the EU across regulatory, economic, and security domains."

The new shape of Russia's digital authoritarianism

Russia's digital trajectory is best understood as a progression through four stages, each building on the previous one. The first stage, from 2012 to 2018, was marked by selective censorship through blacklists, legal pressure and lax enforcement. The second, from 2019 to 2024, shifted towards infrastructure control, as the sovereign internet framework established the legal basis for state-managed traffic control. The third, from 2025 to early 2026, involved whitelist testing and targeted shutdowns, restricting broader connectivity while preserving access to certain approved sites. The fourth, from spring 2026 onwards, has been characterized by systemic degradation, as frequent intervention at the network level has produced tangible collateral damage across banking and public and private services. These stages are cumulative rather than discrete, with earlier mechanisms continuing alongside newer infrastructure controls.

The whitelist shift is particularly important for European analysts because it signals a change in censorship logic from blocking "bad" sites to permitting only approved resources. This logic became clearly visible during the March 2026 shutdowns, when selected state-approved resources remained accessible while broader connectivity failed. Human Rights Watch describes this as an incremental but profound shift that makes it harder for users to bypass restrictions and further narrows the meaning of internet access.[3] In practice, however, even some essential services on the whitelist stopped functioning during the shutdowns, disrupting banks, taxi apps, and government services.[4] Overall, Russia's digital authoritarianism is shifting from controlling content to controlling connectivity itself, while replacing global platforms with domestic alternatives.

3 Human Rights Watch (2026) "Russia: Internet Shutdowns Escalate". 31 March. https://www.hrw.org/news/2026/03/31/russia-internet-shutdowns-escalate.

4 Litvinova 2026.

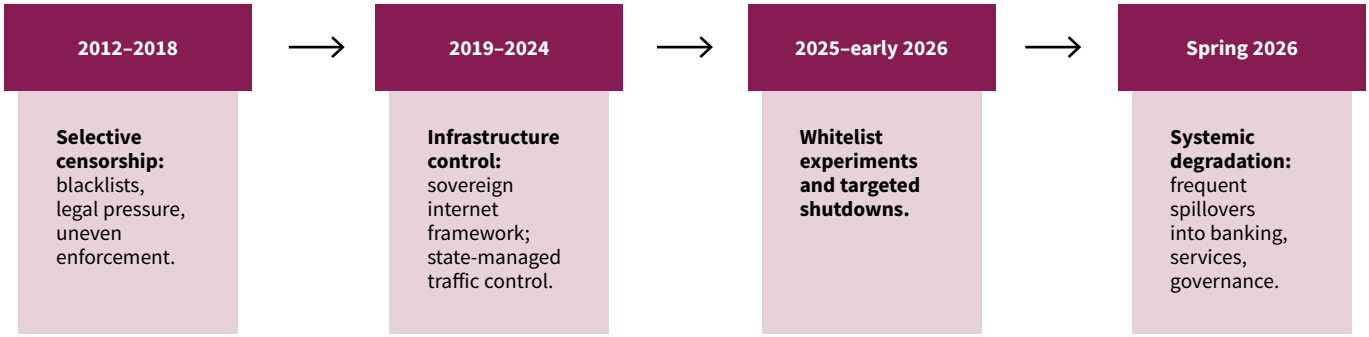

Figure 1. Russia's staged shift towards infrastructure control

Internal costs of digital authoritarianism: The control trap

While tightening digital control may help Putin's regime sustain its war effort in Ukraine in the short term, it comes at high internal and external political costs. The internal costs can be described as a self-reinforcing control trap, in which state responses to perceived risk ultimately undermine the performance of the digital infrastructure and increase long-term infrastructural vulnerability. The trap begins with a perceived threat by the Kremlin – typically political dissent, foreign influence, or information insecurity – which prompts the authorities to impose tighter digital controls, such as filtering, throttling, centralization of routing, and surveillance mandates. While these measures increase short-term visibility and control, they also introduce technical inefficiencies and rigidities, leading to degraded infrastructure performance: slower networks, reduced reliability, and restricted access to services.

As formal systems become less functional, both civilian and institutional users adapt by developing informal workarounds, including both technical solutions and everyday user adaptations such as VPNs, mirror services, grey-market hardware and software, and parallel communication channels. While these adaptations partially restore functionality, they operate outside state oversight, thereby reducing transparency and control. In response, the authorities interpret this circumvention as a renewed risk, triggering further tightening through measures such as deep packet inspection (DPI), blocking tools, and legal penalties. Each iteration intensifies system degradation while increasing dependence on fragile, unofficial solutions that are less secure, less efficient, and harder to regulate. In this way, efforts to consolidate control progressively erode the performance, resilience, and governability of the digital infrastructure itself.

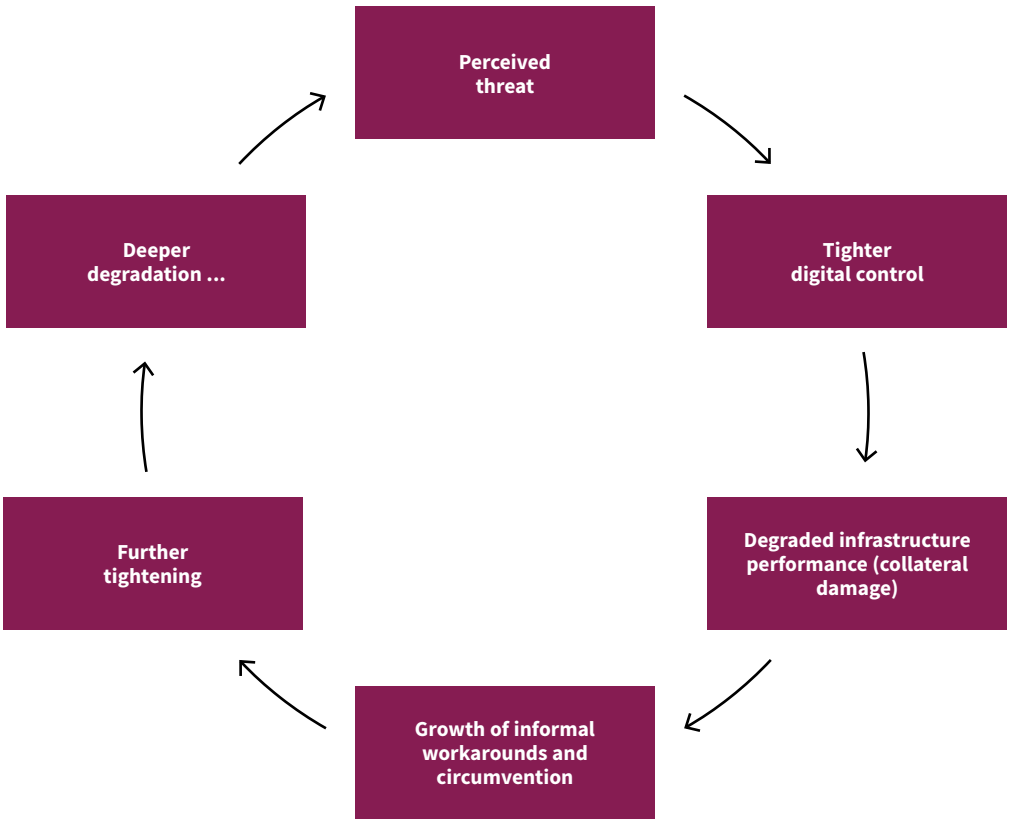

Figure 2. The control trap mechanism

In practice, this control trap mechanism manifests itself in three types of evidence. First, Russia's control architecture is designed to centralize intervention. Deep packet inspection is state censorship equipment that enables the authorities to manipulate internet traffic across thousands of providers.[5] Human Rights Watch also documents that the associated software, EcoSGE, has the capacity to block all traffic except whitelisted websites, even if this capability is not yet routinely used nationwide. This gives the state the technical capacity to move from selective blocking to centralized control over access.

Second, interference at the infrastructure layer produces systemic spillovers. There have been repeated instances of traffic manipulation disrupting access to key services, including the Gosuslugi state services portal, messaging services, and banking applications, with officials attributing disruptions to adjustments or updates in the traffic-control system. In other words, the more the state interferes with the "plumbing" of connectivity, the more it creates failure modes.

Third, the 2026 attack on Telegram – the most popular messaging app used by Russians and owned by Pavel Durov – demonstrates the control trap in policy terms: a service that is seen as politically threatening is also functionally embedded within Russia's wartime society and administration. Telegram is widely used across the Russian state and society, including by Russian soldiers for battlefield communication, as well as by independent media and officials.[6] At the same time, the state promotes domestic alternatives such as Max, but their functionality and adoption remain uneven. This is where state-capacity erosion becomes visible. Excessive control pushes the state towards choices that degrade core governance functions in at least three ways.

First, digital restrictions erode military and coercive capacity. When a widely used communications platform becomes unreliable, actors who rely on speed and coordination, including military personnel and security-linked networks, must switch to slower, less secure, or more fragmented alternatives. Battlefield uses of Telegram, together with the inconvenience that a block creates for ordinary Russians, the armed forces, and businesses, show how embedded the platform is in Russia.[7] The state may ultimately prefer a controlled alternative to Telegram, but the transition costs are significant and can reduce adaptability in a high-tempo wartime environment.

Second, tighter infrastructure control increases financial fragility and payment issues. On 3 April 2026, a large-scale outage affected major Russian banking apps and payment functionality. *Meduza* reported failures in payments, transfers, logins, and ATM cash withdrawals, affecting Sberbank, VTB, and T-Bank, alongside disruptions to the Faster Payments System. *The Moscow Times* similarly reported banking outages amid heightened internet restrictions and pressure on VPN use. Ironically, this has led even staunch regime supporters, such as Natalya Kasperskaya, one of the co-leads of the ultra-conservative pro-state League for a Safe Internet, to raise objections.[8] Whether these failures were directly caused by censorship infrastructure or by broader instability, the key point remains: the regime's further attempts to tighten infrastructure control create systemic risks.

Third, internet shutdowns appear to have contributed to the recent decline in Putin's approval by converting political control into visible economic and everyday disruption. State pollsters recorded a sustained drop in support from above 70% to around 66–68% in March–April 2026,[9] the lowest level since the start of the full-scale war. This decline reflected accumulated discontent over inflation rates and the growing tax burden, as well as internet restrictions, triggering the dip in approval. In April 2026, Russian

5 Human Rights Watch 2026; IT Department (2026, March) "Access Denied: How the Kremlin Controls the Internet — and How to Resist It". Anti-Corruption Foundation (ACF); Epifanova, Alena (2020, January) "Deciphering Russia's 'Sovereign Internet Law': Tightening Control and Accelerating the Splinternet". DGAP Analysis No. 2. German Council on Foreign Relations (DGAP). https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law.

6 Kolomychenko, Maria (2025) "How Far Will the Kremlin Take Its Internet Crackdown?" Carnegie Politika, 16 December. https://carnegieendowment.org/russia-eurasia/politika/2025/12/russia-internet-restrictions.

7 Ibid.

8 *Meduza* (2026) "Natalya Kasperskaya linked banking outages to attempts to block VPNs — and later apologized". 5 April. https://meduza.io/feature/2026/04/05/natalya-kasperskaya-svyazala-sboy-v-rabote-bankov-s-popytkami-roskomnadzora-zablokirovat-vpn-posle-razgovora-s-glavoy-vedomstva-ona-izvinilas.

9 *Meduza* (2026) "Russia's state pollster records 6 straight weeks of declining approval for Putin". 17 April. https://meduza.io/en/news/2026/04/17/russia-s-state-pollster-records-6-straight-weeks-of-declining-approval-for-putin.

lifestyle blogger Viktoria Bonya's viral appeal to Putin illustrated the limits of the Kremlin's strategy: even an apolitical celebrity influencer using banned global platforms can ignite a national debate about internet restrictions and failures in everyday governance. Her campaign exposed how service substitution does not eliminate demand for open channels, but instead politicizes the gap between official claims of digital sovereignty and users' lived experience.

The authoritarian state is simultaneously digitalizing government delivery while building an intervention architecture that can make that delivery unreliable under stress. This is the logic of the control trap: repression drives centralization, centralization produces brittleness, and brittleness motivates more control.

External costs of digital authoritarianism: The sovereign internet and dependence on China

Beyond its domestic costs, Russia's drive for digital sovereignty is deepening a structural trade-off between greater internal control and reduced external freedom of action. Efforts to achieve sovereignty through control are, in practice, generating new forms of external dependence, above all through supply chains linked to China. The paradox is clear: more control at home, less autonomy abroad.

Russia's sovereign internet framework – legally anchored in the 2019 Sovereign Internet Law, which enables centralized network management, the installation of traffic-control equipment, and the development of a national Domain Name System (DNS) – was designed to increase state control over connectivity.[10] Yet its implementation has coincided with growing reliance on external inputs, most notably from China. Russia's imports from China increased from 23% of its total imports in 2021 to 57% in 2024, while China's own dependence on Russia remains limited. This asymmetry leaves Moscow structurally exposed.[11]

This dependency extends beyond consumer goods. Dual-use technologies, such as precision machinery, electronics, and navigation equipment, became a key channel of support, with Chinese exports to Russia exceeding USD 5 billion per month in 2023 before declining in 2024 under stronger secondary-sanctions pressure. China itself remains dependent on European imports in many of these categories. EUISS estimates that in 2024, the EU accounted for at least 30% of China's imports in over one-third of dual-use product categories, worth more than USD 57 billion. This creates a structural constraint on Beijing's ability to sustain large-scale re-exports to Russia.

China's role is therefore not static. It acts as a strategic intermediary whose behaviour is responsive to external pressure, as evidenced by the decline in exports of dual-use components and electronics following sanctions on Chinese financial institutions. At the same time, Russia functions as a high-risk testing ground for China: the deployment of shutdowns, whitelists, and national DNS systems offers observable stress tests of infrastructure-based control under wartime conditions, thereby facilitating authoritarian learning. For the EU, this creates a policy lever, as cooperation increasingly tilts in China's favour and may conflict with Russia's technological ambitions.

Europe's most exposed vulnerabilities

Russia's domestic digital-control capabilities matter for Europe because they intersect with European vulnerabilities at three levels: critical infrastructure, regional spillovers, and global norm-setting.

Critical infrastructure is the most visible and familiar area of vulnerability for the EU. Submarine cables, which carry 99% of intercontinental internet traffic, are increasingly treated as security assets. The European Commission has responded with a Cable Security Toolbox and €347 million in investments to strengthen resilience and repair capacity, while NATO's Baltic Sentry initiative reflects a parallel shift towards protecting undersea infrastructure against destabilizing acts.[12] Satellite navigation systems

10 Epifanova 2020.

11 Caruso, Alessia and Rühlig, Tim (2025) "The dependence gap in Russia–China relations". EUISS. https://www.iss.europa.eu/publications/analysis/dependence-gap-russia-china-relations.

12 European Commission (2026) "Submarine Cable Security Toolbox and Cable Projects of European Interest". https://digital-strategy.ec.europa.eu/en/library/submarine-cable-security-toolbox-and-cable-projects-european-interest.

present another vulnerability. These risks interact directly with Russia's digital-control trajectory. The same state capabilities used domestically to manipulate connectivity – signal interference, traffic control, and infrastructure-level filtering – can also generate trans-border effects. In this sense, the infrastructures of digital authoritarian control and hybrid-threat activity increasingly overlap.

Regional spillovers form the second layer of vulnerability. Infrastructure and governance models diffuse across borders, and authoritarian states use digital technologies both to consolidate control and export surveillance practices to less resilient systems. Russia and China have developed complementary roles in this process: China as a supplier of surveillance infrastructure, and Russia as a provider of lower-cost information manipulation and coercive governance practices.[13] Regional spillovers are not only normative but also embedded in physical and logical infrastructure. Evidence from Central Asia, Eastern Europe, Latin America, the Middle East, and Africa shows that Russian-origin surveillance systems, such as the System for Operative Investigative Activities (SORM),[14] have been widely adopted, often serving as a baseline for national monitoring capabilities.[15] For the EU, this creates a near-abroad environment where sovereignty-first digital governance becomes entrenched, reducing resilience and constraining information pluralism.

The third dimension is global norm-setting. The current contest over who will shape digital norms beyond Europe will determine the new rules of the game. Its outcome will influence whether Moscow's repressive approach to internet regulation and China's state-centric cyber sovereignty gain ground around the world as new international norms, or whether the EU's rights-based and interoperable model of the internet will prevail. This divide is increasingly visible in international forums, where Russia and China actively promote sovereignty-first approaches to internet governance and challenge the multi-stakeholder model.[16]

"A coherent EU response to Russia's infrastructure-based digital authoritarianism requires moving beyond a sanctions-only approach towards a more holistic security strategy that integrates resilience, enforcement, and normative leadership."

Conclusions: EU policy priorities and levers

A coherent EU response to Russia's infrastructure-based digital authoritarianism requires moving beyond a sanctions-only approach towards a more holistic security strategy that integrates resilience, enforcement, and normative leadership.

First, connectivity must be treated as critical infrastructure. The EU is moving towards stricter requirements for removing high-risk suppliers from 5G networks, signalling a transition from voluntary guidance to mandatory risk reduction. EU initiatives on submarine cable security and NATO's protection of undersea assets reflect the same trend, linking physical infrastructure security to broader digital resilience. However, this logic needs to be expanded further, for instance by tightening regulation of

13 Sinkkonen, Elina & Lassila, Jussi (2020) "Digital Authoritarianism in China and Russia: Common Goals and Diverging Standpoints in the Era of Great-Power Rivalry". *FIIA Briefing Paper* 294, October 2020, The Finnish Institute of International Affairs. https://fiia.fi/en/publication/digital-authoritarianism-in-china-and-russia.

14 SORM is Russia's state-mandated surveillance system, which provides security services with direct, real-time access to telecommunications and internet traffic through equipment installed within network infrastructure.

15 Bourgelais, Peter (2013) "The 'Commonwealth of Surveillance States': The Export of Russian Surveillance Technologies". Access Now. https://www.accessnow.org/wp-content/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf; Recorded Future (2025) "Tracking the Deployment of Russian Surveillance Technologies in Central Asia and Latin America". Insikt Group. https://www.recordedfuture.com/research/tracking-deployment-russian-surveillance-technologies-central-asia-latin-america.

16 Polyakova, Alina & Meserole, Chris (2019) "Exporting Digital Authoritarianism: The Russian and Chinese Models". Brookings Institution. https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf; Lucenti, Flavia & Saari, Sinikukka (2025) "Russia's Multilateral Cyber Norm Promotion: The Duality of Great Power Projection and Digital Authoritarianism". *Geopolitics*, 1–25. https://doi.org/10.1080/14650045.2025.2601982.

AI training data. From this perspective, the EU's engagement with platform gatekeepers remains critical, particularly regarding the availability of circumvention tools in app distribution.

Second, China's ability to supply Russia, particularly with dual-use technologies, remains partly dependent on EU-origin inputs. Targeted enforcement, including secondary sanctions, has already contributed to the decline in Chinese exports to Russia. Strengthening controls on transshipment pathways can further raise the cost of sustaining Russia's digital-control infrastructure.

Third, more consistent and conditional support for secure, rights-preserving connectivity tools, combined with the use of sanctions, should be treated as a strategic security instrument. Viewing such support as a purely humanitarian measure is a strategic mistake. Russia's censorship architecture explicitly targets VPNs and circumvention technologies. Expanding secure communications, independent media access, and diversified circumvention tools strengthens both societal resilience and the EU's normative influence.

Fourth, given the diffusion of surveillance and governance models, the EU should prioritize resilience-building in neighbouring states. The region functions as a leading indicator: practices normalized there can shape future governance environments closer to the EU. This is not only a matter of sustaining democracy, but also of security.

Internet governance is now a site of long-term geopolitical competition. Russia and China promote sovereignty-first models, aiming to reshape global norms. At the same time, EU policy should aim to amplify trade-offs between control and functionality within Russia's system.

BRIEFING
PAPER
436
May 2026

ISBN 978-951-769-856-6
ISSN 1795-8059
Language editing: Lynn Nikkanen
Graphics: Joonas Juutilainen
Cover photo: Hector Retamal / AFP / Lehtikuva

FIIA
FINNISH
INSTITUTE OF
INTERNATIONAL
AFFAIRS

Arkadiankatu 23 b
POB 425 / 00101 Helsinki
Telephone +358 (0)9 432 7799
www.fiia.fi