GSSC
GEOPOLITICS AND SECURITY STUDIES CENTER

COUNTERING FOREIGN INFORMATION MANIPULATION IN THE BALTIC SEA REGION:

PATTERNS, RESPONSES AND GAPS

Funded by

Svenska institutet

In partnership with

Embassy of Sweden
Vilnius

The views expressed in this publication are those of the authors and do not necessarily reflect the position of GSSC or its partners.

2026

Content

Introduction 4

Nerijus Maliukevičius
Russian Influence Operations and Resilience in Lithuania 7

Una Aleksandra Bērziņa-Čerenkova
Malign Information Influence in Latvia 2020–2025: Unchanged Goals yet Evolving Playbooks 16

Marek Kohv
Mapping Russian Disinformation in Estonia 23

Jussi Lassila
Russian Information Influence on Finland Before 2022 and Prospects Afterwards 29

Martin Kragh
Russian Influence Operations Towards Sweden 34

Jeanette Serritzlev
Russian Disinformation in Denmark 38

Nikolai Klimeniouk
Too Little, Too Late: Germany's "Take It Easy" Approach to Russian Hybrid Warfare 43

Laurynas Vaičiūnas
Russia's Narratives in Poland and Their Local Instigators 50

Conclusion 56

Introduction

Dominykas Nedzinskas

Project Manager at the Geopolitics and Security Studies Center

This report analyses the changing role of Russian information operations across Lithuania, Latvia, Estonia, Finland, Sweden, Denmark, Germany, and Poland, bringing together eight country-focused studies into a single analytical policy paper. It examines how the Russian Federation and other actors use propaganda and disinformation as part of a broader strategy of influence, presenting both the techniques and channels employed as well as the dominant narratives tailored to respective country's context. In doing so, the report provides a comparative perspective (see Summary), identifying not only cross-country similarities but also the ways in which influence operations are adapted to local political, social, and informational environments. It places Russian activities alongside the growing, though distinct, influence efforts of other authoritarian actors such as Belarus and China, whose approaches differ in scale, scope, intensity, and intent but increasingly overlap within the same information space.

The growing importance of information as a tool of state power is not accidental. In 2013 already, General of the Army Valery Gerasimov, Chief of the General Staff of the Russian Federation Armed Forces, argued that the "rules of war" were changing, with non-military means, especially information, becoming key to achieving strategic goals.[1]

This way of thinking has since become deeply embedded in Russian political and military discourse. It shows a broader understanding of conflict in which influencing debates and opinions, as well as weakening opponents' societal unity can be as effective as the use of military force. These ideas have been further reflected in official doctrinal documents of the Russian Federation[2 3] and echoed by influential figures within Russia's state-controlled media ecosystem, including RT (Russia Today) editor-in-chief Margarita Simonyan,[4] who has openly advocated for the importance of information warfare.[5]

Over the past two decades, Russia has steadily developed this approach. What began as a relatively fragmented set of influence activities in the early 2000s, has evolved into a more coordinated and adaptive system. Key turning points were the colour revolutions in Yugoslavia, Georgia, Ukraine, and Kyrgyzstan, as well as the Russo-Georgian War, which once again reinforced the Kremlin's view that information space is a critical arena of competition.[6] Since then, the Kremlin has invested heavily in its global communication capabilities, most visibly through launching state-backed outlet RT,[7] but also through a wide range of less visible and obvious channels to better its image and "tell its own story".

While Russian information activities are global, they are particularly pronounced in Northern, Central, and Eastern Europe. These regions are not only geographically close to Russia but also politically and historically significant, making them especially relevant targets for influence operations. For example, Lithuania, Latvia, and Estonia, as well as Poland, are still often referred to as the "blizhneye zarubezhye" ("near abroad") — a term showing that Moscow still considers these countries as belonging to its sphere of influence. Adding to that, since the full-scale invasion of Ukraine, these efforts have intensified further, with many analysts noting a sharp increase in both the volume and sophistication of disinformation campaigns. National threat assessments across the eight selected countries consistently identify Russia as the primary or at the very least, one of the two most serious adversaries, with little indication that this will change in the near term, instead signalling toward a sustained, coordinated, and adaptive long-term challenge.

What makes the current Russian influence operations unique is its combination of continuity and adaptation. Many techniques—such as narrative framing, the use of proxies, and the exploitation of social divisions, have clear roots in Soviet-era practices[8]. At the same time, these old methods are now reinforced by modern technologies, for example by algorithm-driven amplification, coordinated online behaviour (bots), and the use of artificial intelligence. Recent campaigns like " Doppelgänger" showed how these tools can be used to imitate credible sources and blur the line between authentic and manipulated content. The scale and sophistication of such operations make this analysis particularly timely, as "Doppelgänger" is widely considered one of the most extensive and impactful pro-Russian disinformation campaigns identified to date[9] Meta has classified "Doppelgänger" as an advanced persistent threat (APT) and emphasised the campaign's adaptability and longevity.[10]

Across the countries examined in this report, Kremlin influence operations rarely rely on a single message or narrative. Instead, they work by affecting the whole information environment by creating confusion, uncertainty, and gradually eroding trust. Rather than attempting to persuade audiences of a specific version of reality, contemporary Russian propaganda increasingly seeks to erode the very idea of objective truth. In contrast to Soviet-era propaganda, which goal was to demonstrate the correctness and superiority of its claims, current Kremlin communication operates on a more relativistic logic—suggesting that truth is subjective, contingent, and dependent on perspective. By creating ambiguity and competing interpretations, these actions make it harder to distinguish fact from fiction, while simultaneously exploiting existing societal tensions related to history, identity, economic pressures, or migration.

For this reason, the report treats propaganda not as isolated messages, but as a systemic practice that has evolved from persuasion toward the deliberate production of doubt and epistemic uncertainty. Despite differences in methods across countries, the objectives are widely assessed to include weakening trust in democratic institutions, undermining support for Ukraine and Euro-Atlantic cooperation, and deepening social divisions. These efforts also tend to intensify during periods of crisis, such as elections or economic shocks, when societies are more vulnerable to manipulation.

Under these circumstances, the report not only explains how Russian information influence works, but also how different countries respond to it. It analyses national approaches ranging from institutional coordination and strategic communication to media literacy and legal measures, showing both strengths and persistent gaps. By comparing these experiences, the report identifies lessons for strengthening resilience at both national and regional levels.

Purpose and Research Questions

This policy paper builds on the country studies by taking a comparative approach to hostile information influence in these countries. Its focus is not limited to narratives alone but extends to the broader ecosystem in which influence takes place — covering actors, channels, and techniques. The aim is to better understand how coordinated Russian influence operations shape the public debate, use vulnerabilities, and affect resilience of the society.

Several key questions guide the analysis:

- How do contemporary techniques—such as coordinated amplification or AI manipulation affect societal vulnerability?
- How are narratives embedded within specific political, historical, and linguistic contexts?
- How do influence operations contribute to broader hybrid strategies aimed at fostering distrust, polarisation, and decision-making paralysis?
- What steps can countries take to move from reactive responses toward more proactive and systemic approaches, including whole-of-society resilience models and early-warning mechanisms?

The report also places national experiences within a wider regional perspective. While each country faces distinct challenges, many of the dynamics are shared. By comparing how states identify threats, organise responses, and build resilience, the paper highlights opportunities for closer coordination and mutual learning. In doing so, it gives practical recommendations to strengthen collective defence against information threats and to scale effective countermeasures across the region.

References

1. Military Review. 2016. The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf

2. Russian Federation 2016. Doctrine of Information Security of the Russian Federation. Approved by Presidential Decree No. 646, December 5, 2016. http://www.scrf.gov.ru/security/information/DIB_engl/

3. Russian Federation. 2021. Основы государственной политики Российской Федерации в области международной информационной безопасности. Утверждены Указом Президента Российской Федерации от 12 апреля 2021 г. № 213. https://www.mid.ru/ru/foreign_policy/official_documents/1871845/

4. Azar, I. 2013. 'Не собираюсь делать вид, что я объективная'. Интервью с Маргаритой Симоньян. Lenta.ru, 7 March. https://lenta.ru/

5. Darczewska, J. 2025. Capturing Minds and Reshaping the World. Ośrodek Studiów Wschodnich (OSW). https://www.osw.waw.pl/en/publikacje/osw-report/2025-12-30/capturing-minds-and-reshaping-world

6. Christopher, P. and Matthews, M. 2016. The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation. https://www.rand.org/pubs/perspectives/PE198.html

7. U.S. Department of State Global Engagement Center. 2022. Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem. https://2021-2025.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf

8. Giles, Keir, 2016. Handbook of Russian Information Warfare. NATO Defense College. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf

9. Federal Foreign Office (Germany). 2024. Technical Report on an Analysis by the Federal Foreign Office – Germany Targeted by the Pro-Russian Disinformation Campaign 'Doppelgänger'". https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf

10. Meta. 2025. Adversarial Threat Report, Fourth Quarter. https://transparency.meta.com/sr/Q4-2024-Adversarial-threat-report/

Russian Influence Operations and Resilience in Lithuania

Dr. Nerijus Maliukevičius

Associate Professor at the Institute of International Relations and Political Science (Vilnius University)

This Lithuanian case study outlines how malign propaganda and disinformation narratives are spread within the information ecosystem and employed to undermine societal cohesion as well as trust in democratic institutions and security alliances. The chapter traces the evolution of Russia's influence operations from narrative manipulation to more aggressive physical attempts to shape Lithuania's political and security agenda in ways that serve the Kremlin's interests. It presents concrete examples of diversionary operations, enabling a clearer understanding of how Moscow's modus operandi is evolving. The chapter further examines the resilience practices Lithuania has developed in response to these threats, with particular attention given to the evolution of a whole-of-society model that integrates state institutions, legal frameworks, civic initiatives, media actors and international cooperation.

Structure and Dynamics of Hostile Narratives Targeting Lithuania

The information ecosystems of contemporary societies are predominantly shaped by digital platforms and social networks. Propaganda and disinformation have emerged as a persistent instrument of malign authoritarian influence in this new media realm. Such ecosystems are increasingly exploited to spread and amplify hostile narratives that polarise societies and weaken trust in democratic governance and processes. This analysis of the Lithuanian case draws on a purpose-built "Human-Annotated Lithuanian Textual Corpus for Propaganda Narratives and Techniques" (HALT-PROP) (Rizgelienė et al., 2026). The corpus comprises 1,000 Lithuanian-language media texts published between 2018 and 2024, selected from a broader pool of content originating from a range of information sources, including openly hostile platforms and a national public media outlet (LRT.lt), used as a control sample.

Source/ media outlet	Number of items collected	Number of items after filtration
Būkimevieningi.lt	7,409	6,787
Ekspertai.eu	13,052	10,367
Infa.lt	6,996	6,491
Komentaras.lt	1,893	1,403
Ldiena.lt (ldiena.com)	18,416	15,583
Lrt.lt	139,845	133,197
Minfo.lt	15,880	15,530
Total:	203,491	186,376

Table 1. Media outlets selected to provide texts for the HALT-PROP dataset (Rizgelienė et al., 2026)

The dataset was designed to enable the systematic study of propaganda and disinformation not as isolated messages, but as a structured and recurring phenomenon within the Lithuanian information environment. All source material was collected using automated methods, resulting in an initial dataset of more than 200,000 media items (Rizgelienė et al., 2026).

From this larger corpus, texts were filtered, and a subset of 1,000 articles was selected for in-depth analysis based on predefined criteria for propaganda. Specifically, selected articles had to employ at least one identified propaganda technique and articulate a hostile or malign narrative directed against the Lithuanian state, its institutions or its international alliances. Each text was manually annotated for propaganda techniques and narratives, allowing for a dual-level analysis of how influence is constructed and what propaganda content it conveys (Zubaitienė et al., 2025).

The analysis of Russian propaganda narratives targeting Lithuania draws on the methodological framework proposed by Catherine Kohler Riessman, which distinguishes between core thematic narrative structures and

the rhetorical techniques used to amplify and legitimise them (Riessman, 2005). The first analytical level focuses on narrative content – what is said – while the second examines how it is said, that is, how narratives are constructed and which propaganda techniques are used. The 2018 NATO Strategic Communications Centre of Excellence report "Russia's Footprint in the Nordic-Baltic Information Environment" identified 29 recurring narratives targeting the Nordic–Baltic region (Bērziņa et al., 2018), while a follow-up study in 2020 further refined this typology by consolidating, adding and discarding specific narratives (Cepurītis et al., 2020). The list of narratives was complemented by Lithuania's Annual National Threat Assessment, which consistently highlights a stable core of narratives promoted by Russia, i.e. the delegitimisation of Western sanctions, hostility towards Ukrainian refugees, claims of imminent war in the Baltic states, the alleged futility of supporting Ukraine and assertions that the war in Ukraine is irrelevant to Western interests (NTA, 2023; 2024; 2025).

On this basis, the annotation framework operationalised eleven analytically distinct but interrelated narrative categories reflecting both continuity and adaptation in hostile messaging patterns.

No.	Narrative category	Analytical description
1	**Disinformation about the war in Ukraine**	Spreading false or misleading narratives to justify Russia's aggression and delegitimise Ukrainian resistance.
2	**Delegitimisation of the Lithuanian State**	Portraying Lithuania as a failed or artificial "project", questioning its sovereignty and historical foundations.
3	**Undermining the Lithuanian Armed Forces**	Attacks on military funding, modernisation and NATO deployments, framing Lithuania as militaristic or provocatively anti-Russian.
4	**Erosion of trust in Lithuanian institutions**	Depicting state authorities as corrupt, incompetent or unrepresentative.
5	**Attacks on Western institutions and alliances**	Discrediting the EU, NATO and other multilateral bodies as exploitative, ineffective or morally bankrupt.
6	**Decline of Western civilisation**	Claims of Western moral decay, often emphasising gender ideology, LGBT rights and secularism in contrast to "traditional values".
7	**Authoritarian model promotion**	Presenting regimes such as Russia, Belarus or China as stable, efficient and sovereign alternatives to Western democratic "chaos".
8	**Narratives of US decline and "Washington hegemony"**	Framing the US as a waning imperial power and promoting the idea of a multipolar world order.
9	**Geopolitical reordering and the "New World Order"**	Promoting conspiracy-laden narratives of global realignment, replacing liberal democratic systems with authoritarian alliances.
10	**Weaponisation of migration and refugees**	Amplifying fears of migration and portraying refugees as tools of hybrid warfare or existential threats to national identity and security
11	**Revival of "Litvinism"**	Using historical revisionism to claim parts of Lithuania historically belonged to Belarus, undermining national identity and territorial integrity.

Table 2. Russian propaganda narratives targeting Lithuania (Rizgelienė et al., 2025)

The empirical distribution of narratives in the annotated corpus of 1,000 articles confirms that Russian influence operations targeting Lithuania are structurally oriented towards the erosion of institutional trust rather than isolated issue-based messaging.

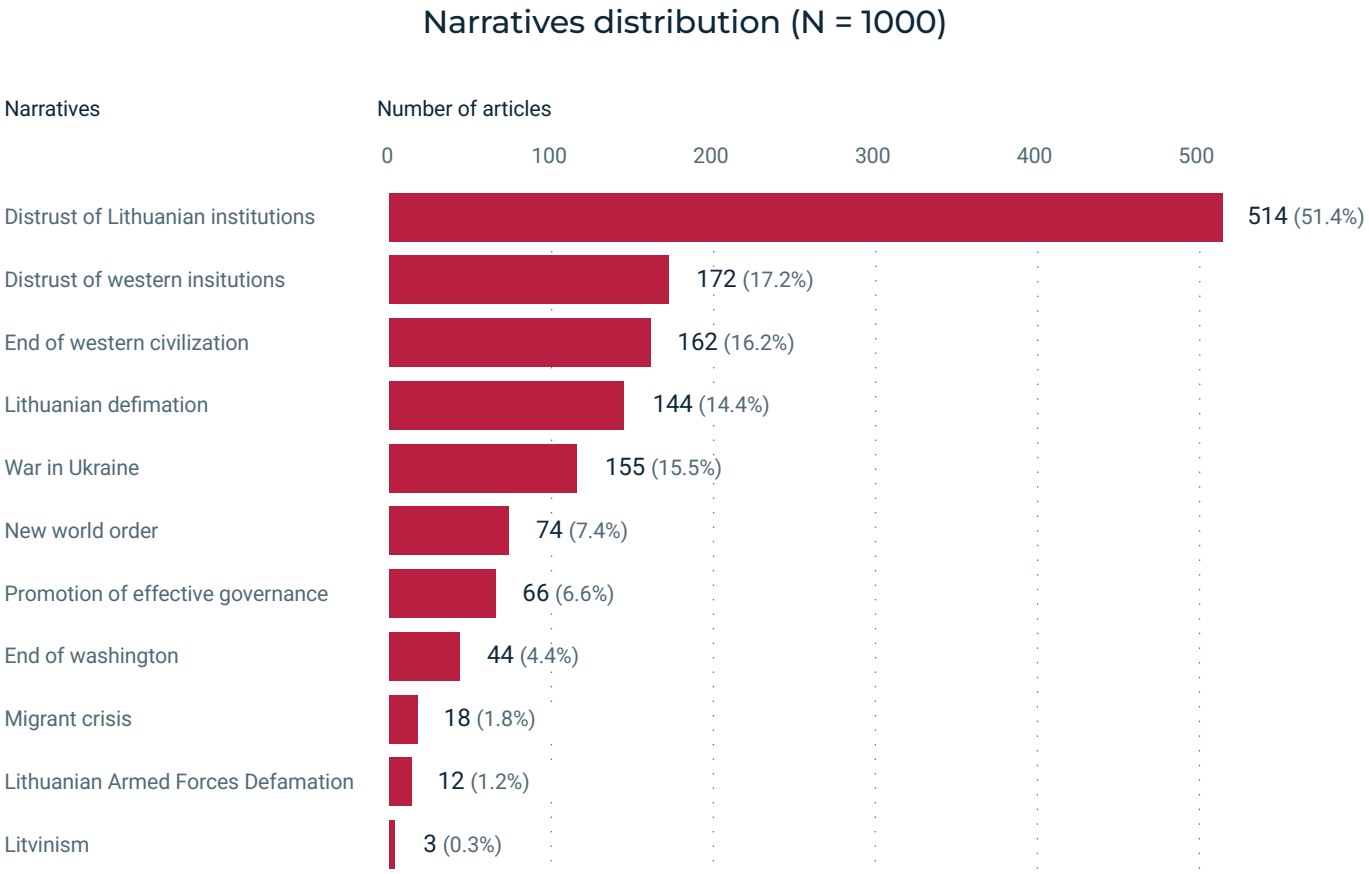


Figure 1. Narratives distribution (author: Ieva Rizgelienė)

As shown in Figure 1, narratives aimed at undermining Lithuanian institutions constitute the dominant thematic cluster, accounting for more than half of all analysed articles (51.4%) in the corpus. This finding empirically substantiates the strategic priority placed on delegitimising the Lithuanian state and its governance capacity, consistent with long-standing Russian strategy. A second group of narratives targets Western institutions and alliances (17.2%), promotes claims about the decline of Western civilisation (16.2%) and defames Lithuanian statehood (14.4%). Together, these narratives reinforce a broader meta-frame in which Lithuania is portrayed as dependent on, and ultimately betrayed by, a failing Western political and moral order. Narratives directly related to the war in Ukraine (11.5%) appear less frequently as standalone themes but function as an important supporting layer that legitimises Russia's aggression and reframes Lithuania's security posture as irrational or provocative.

The co-occurrence analysis further demonstrated that malign narratives rarely operate in isolation. Only a limited number of texts from openly hostile media platforms relied on a single narrative frame. Instead, dominant narratives – particularly the erosion of trust in Lithuanian institutions, the decline of Western civilisation and the delegitimisation of Western governance – were systematically embedded within multi-narrative constructions. Such a pattern indicates a deliberate strategy of thematic stacking, in which institutional distrust is further amplified through civilisational, geopolitical and historical arguments.

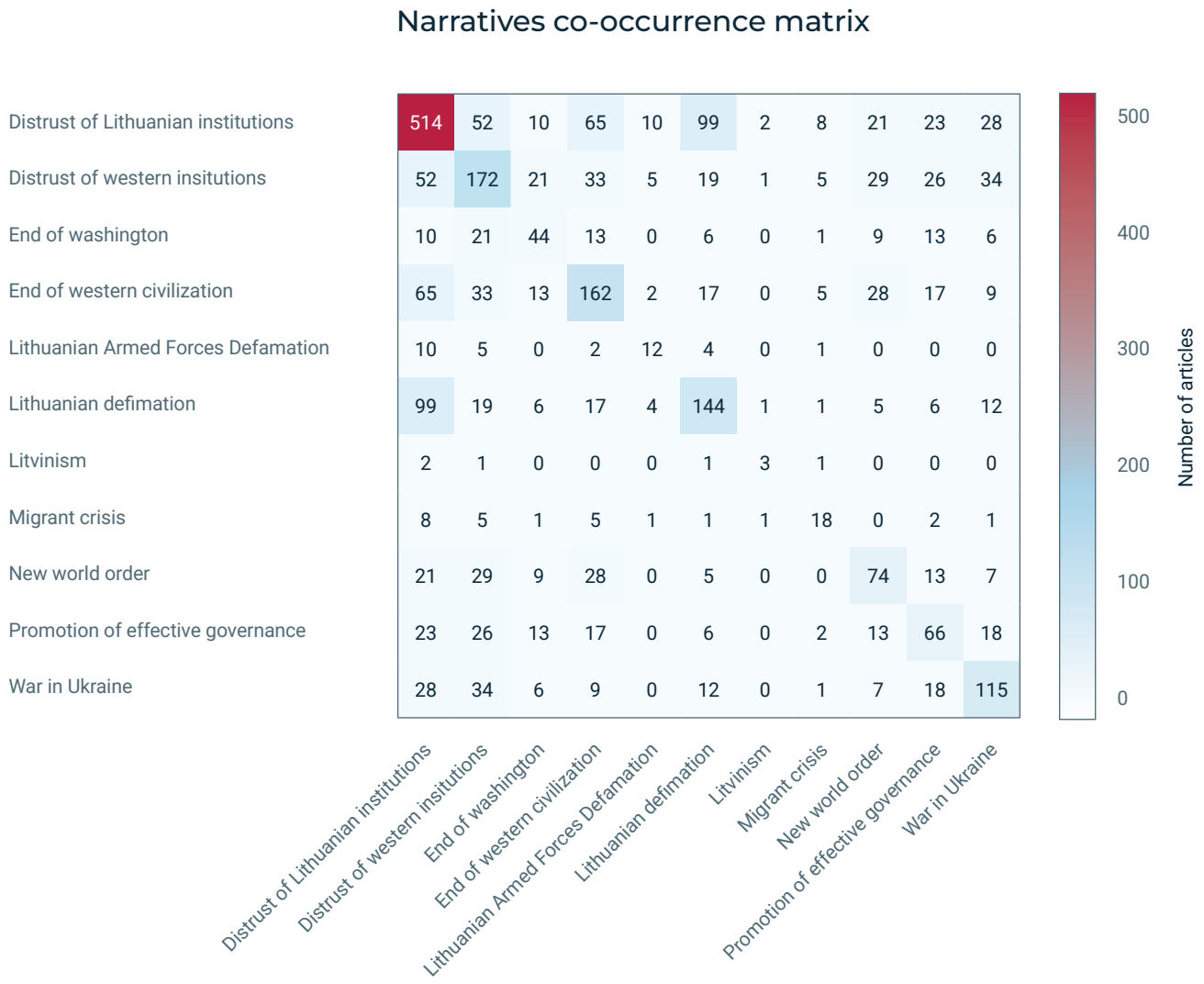


Figure 2. Narrative co-occurrence matrix (author: Ieva Rizgelienė)

The narrative co-occurrence matrix (Figure 2) reveals particularly strong linkages between the delegitimisation of Lithuanian institutions and the defamation of Lithuania, as well as recurring overlaps with Western institutional distrust and "end of Western civilisation" narratives. These combinations suggest a coherent narrative architecture aimed at reframing Lithuania as simultaneously internally corrupt, externally controlled and geopolitically doomed. By contrast, more marginal narratives – such as Litvinism, migration weaponisation and defamation of the Lithuanian Armed Forces – appear infrequently and almost exclusively alongside dominant frames, indicating their supporting role in reinforcing broader delegitimisation strategies.

If narratives define the content of influence operations, propaganda techniques determine their affective force. Following the analytical path proposed by Riessman, it is important to proceed from thematic (narrative) analysis to an examination of style and propaganda techniques. Based on the literature of propaganda studies (Hobbs and McGee, 2014), a set of ten analytically distinct propaganda techniques was identified, capturing mechanisms of emotional mobilisation and argumentative distortion.

No.	Technique	Analytical description
1	**Emotional expression**	Deliberate use of emotionally charged language (e.g. fear, anger, pride, sympathy) to provoke strong affective responses and influence attitudes or behaviour. Often substitutes emotional appeal for evidence-based reasoning and relies on exaggeration, personal attacks and vague but positively connoted terms.
2	**Whataboutism / red herring / straw man**	Diverts attention from the central issue by shifting blame to others (whataboutism), introducing irrelevant topics (red herrings) or misrepresenting an opponent's position to attack a weakened or distorted version of it (straw man). Used to deflect criticism and avoid substantive engagement.
3	**Simplification**	Reduces complex political or social issues to overly simplistic explanations by attributing responsibility to a single cause, group or binary opposition. Employs clichés and slogans that discourage critical analysis and obscure structural complexity.
4	**Intentional vagueness (obfuscation)**	Uses ambiguous, imprecise or abstract language to obscure meaning, enable multiple interpretations and evade accountability or factual verification.
5	**Appeal to authority**	Legitimises claims by referencing perceived authoritative figures or institutions without providing verifiable evidence, implying truth based on status rather than substantiation.
6	**Flag-waving**	Promotes a position by invoking patriotism, national pride or loyalty to the state, suggesting alignment with national interests regardless of factual accuracy or rational justification.
7	**Bandwagon**	Encourages conformity by implying that a belief or behaviour is widely accepted or represents the majority view, leveraging social pressure and fear of exclusion.
8	**Doubt/smears**	Undermines credibility by casting suspicion or attacking character – either indirectly through insinuation (doubt) or directly through unsubstantiated accusations (smears) – without presenting any concrete evidence.
9	**Reduction ad Hitlerum/Stalinum**	Discredits individuals, ideas or groups by associating them with historically vilified figures (e.g. Hitler, Stalin), relying on emotional shock rather than addressing substantive arguments.
10	**Repetition**	Reinforces messages through frequent repetition, increasing perceived truthfulness over time, even in the absence of evidence – a cognitive bias known as the "illusion of truth" effect.

Table 3. Classification and description of common propaganda techniques (Rizgelienė et al., 2025)

These techniques were operationalised as identifiable discursive features and systematically applied to the corpus of 1,000 manually annotated articles (Zubaitienė et al., 2025). Each text was coded for the presence and co-occurrence of specific techniques, allowing the analysis to move beyond isolated rhetorical devices and assess broader stylistic patterns.

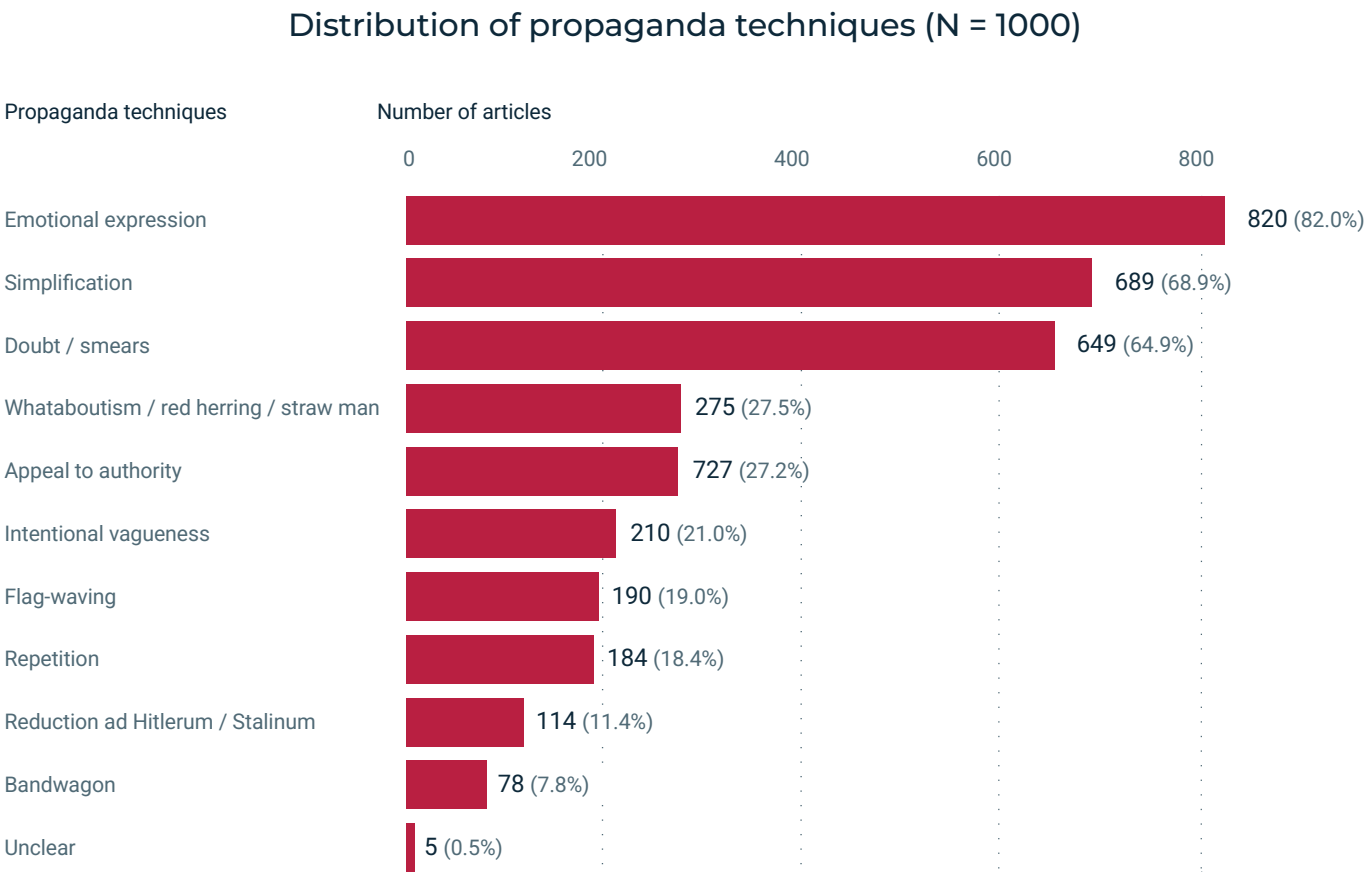


Figure 3. Distribution of propaganda techniques (author: Ieva Rizgelienė)

The frequency of use of the various propaganda techniques (Figure 3) reveals a clear stylistic hierarchy in hostile messaging. Emotional expression is by far the dominant technique, present in 82.0% of analysed articles, confirming the central role of affective mobilisation in malign influence operations. Rather than persuading through arguments, hostile actors prioritise fear, anger, resentment and moral outrage as primary mechanisms of engagement. This emotional core is systematically reinforced by simplification (68.9%) and the use of doubt and smears (64.9%), indicating a strategy that simultaneously reduces political complexity to binary frames and undermines trust in institutions, individuals and democratic processes. A secondary layer of techniques – whataboutism and related diversionary tactics (27.5%), appeal to authority (27.2%) and intentional vagueness (21.0%) – shields emotionally charged claims from scrutiny by deflecting responsibility and obscuring causal links. More explicit mobilisation devices, such as flag-waving (19.0%), repetition (18.4%) and bandwagon appeals (7.8%), appear less frequently but contribute to message reinforcement and perceived consensus. Extreme delegitimisation strategies, including reduction ad Hitlerum (11.4%), remain marginal yet symbolically potent and are selectively deployed to provoke moral shock. Overall, the pattern demonstrates that Russian propaganda targeting Lithuania relies less on coherent ideological argumentation than on a layered stylistic structure in which emotional saturation, simplification and systematic distrust-building operate in tandem to normalise hostile narratives and erode societal resilience.

The analysis of the corpus of Lithuanian-language media texts published on openly hostile platforms between 2018 and 2024 demonstrates that Russian propaganda targeting Lithuania is not organised around episodic themes, but around a stable core of institutional-erosion narratives. This helps explain the resilience challenge faced by democratic societies: influence operations are designed not merely to persuade, but to saturate the information environment with mutually reinforcing narratives that normalise distrust and democratic backsliding.

From Narrative Saturation to Covert and Kinetic Escalation

While hostile narratives and propaganda techniques constitute the foundational layer of Russian influence operations, the Lithuanian case demonstrates that over time, narrative saturation and institutional delegitimisation have increasingly been complemented by covert, coercive and ultimately kinetic actions. This evolution reflects a broader shift in Russian strategic practice from reliance on soft-power instruments towards the use of sharp and dark power (NED, 2017; Galeotti, 2020), including sabotage, intimidation and proxy-based violence. In this logic, information operations function not only to shape perceptions but also to prepare a permissive informational environment for deniable physical actions aimed at testing institutional resilience, intimidating society and disrupting support for Ukraine.

Following Russia's full-scale invasion of Ukraine on 24 February 2022, the character of Russian influence operations targeting Lithuania underwent a qualitative transformation. Developments over recent years indicate that informational influence has increasingly been accompanied by physical and kinetic actions. Journalists have documented that Russia's "covert war" against Europe encompasses coordinated physical attacks against critical infrastructure, logistical chains supporting Ukraine, and sites of symbolic importance to national identity and historical memory (LRT, 2025a). Lithuania, in this broader European pattern, appears not as an isolated case, but as one of the operational environments in which such activities were detected at an early stage and traced to Russian intelligence services.

One of the most revealing cases identified through international investigative reporting exposed Vilnius as a logistical and coordination node within a wider network of Russian intelligence activities. The investigation demonstrated that explosive materials, sabotage-related equipment, and operatives were moved through Lithuania towards other European states, with operations deliberately concealed within civilian logistics systems, including courier services and commercial shipments (LRT, 2025b).

Alongside logistical and infrastructural targeting, Russian-linked operations have also employed symbolic acts of violence aimed at reinforcing long-standing disinformation narratives. Attacks against sites of historical memory serve a dual function: they operate as physical intimidation while simultaneously materialising narratives that question Lithuania's historical legitimacy and resistance tradition. The desecration of the monument to partisan commander Adolfas Ramanauskas-Vanagas illustrates this logic. The act cannot be understood solely as vandalism, but as a kinetic extension of earlier narrative campaigns delegitimising Lithuania's post-war resistance and statehood (LRT, 2025c).

The clearest indication of escalation is provided by the attempted terrorist attacks in Šiauliai in September 2024. These actions targeted infrastructure belonging to UAB TVC Solutions, a company that produces mobile radio-frequency spectrum analysis stations intended for use by the Armed Forces of Ukraine. The choice of target reflects a shift towards direct interference with the provision of military assistance to Ukraine through deniable kinetic means. According to the criminal case materials, six individuals were involved in an organised operational structure that conducted reconnaissance, planned arson attacks and attempted to destroy equipment valued at more than four million euros (Prosecutor General's Office of the Republic of Lithuania, 2026). The operational pattern reveals a high degree of coordination and transnationality. The investigation established the involvement of citizens of Spain, Colombia, Russia and Belarus, operating in distinct roles across multiple stages of preparation and execution (Prosecutor General's Office of the Republic of Lithuania, 2026). The case demonstrates a deliberate progression from influence operations to planned acts of terrorism against assets supporting Ukraine's military capacity.

Taken together, these cases illustrate a structural evolution in Russian influence operations targeting Lithuania. Narrative manipulation and propaganda continue to play a central role, but they are increasingly embedded within a broader strategy that incorporates physical disruption, intimidation and the preparation of violent acts. Information operations in this framework serve to normalise hostility, obscure attribution and create a permissive environment in which kinetic actions can be conducted below the threshold of open conflict. The Lithuanian case thus demonstrates how contemporary Russian influence operations operate along a continuum – from cognitive shaping to covert physical action.

Building Resilience Against Hybrid Influence Operations

Lithuania's strategy for countering Russian disinformation is distinguished by its comprehensive approach: not a collection of isolated measures, but a multi-layered, interconnected model. It rests on four core pillars – regulation of the information space, strengthening a professional media environment, fostering civic engagement and developing strategic communication capacities (Maliukevičius, 2024). This multi-layered structure has enabled Lithuania to gradually shift from fragmented, reactive responses to a more systematic posture suited to long-term, complex information threats.

Lithuania's lessons for the wider Nordic–Baltic region suggest that a complex, whole-of-society resilience model is a long-term, gradual process. It is not a single measure

or decision, but a system of interlinked actions based on the four pillars outlined above: regulation reduces systematic dissemination of harmful content, a professional media sustains the supply of reliable information, civic initiatives function as a rapid horizontal response network, and strategic communication ensures coordinated vertical institutional response during crises and information incidents. The interaction between horizontal (civic) and vertical (institutional) components is essential – without it, resilience remains fragmented and slow.

Lithuania's experience also shows that countering external malicious informational influence cannot be framed solely as a "communication" or "media" issue. It is a long-term task of democratic-state protection that includes societal behaviour, institutional decision-making processes and the infrastructure of the information ecosystem. Resilience is therefore built not only by restricting harmful content but also by increasing access to reliable information, developing competencies, ensuring there are appropriate crisis-management algorithms and sustaining consistent international partnerships. This combination of policy measures and societal engagement generates a deterrence effect: it reduces the effectiveness of hostile campaigns, increases their costs and shortens their "lifespan" in the information ecosystem.

This model may be useful to other Nordic–Baltic democracies developing resilience strategies, particularly when confronted with influence operations conducted by authoritarian regimes. The core lesson is the need to invest in capacities that operate not in isolation, but as one system. Strategic communication competencies should be strengthened across all state institutions with adequate financial and human resources, while also incorporating civic initiatives, local communities and digital platforms. In parallel, public education campaigns are needed, not only on general "media literacy" but also on specific skills: recognising disinformation, cybersecurity hygiene, the mechanics of manipulation and conspiracy theories, and responsible information-sharing practices during electoral cycles.

Another key direction is early warning and monitoring. Contemporary disinformation campaigns evolve rapidly, requiring effective monitoring systems, clear response algorithms and timely information exchange with international partners. This domain is not only technological, institutional readiness matters as well – who assesses an incident, who decides on the form of response, when a public response is warranted and when a strictly internal inter-institutional response is preferable to avoid artificially amplifying a hostile narrative.

Resilience also depends on the security of media infrastructure. Media and information-distribution infrastructure should be treated as part of critical infrastructure, and its cyber security as a national security issue. Hostile actors systematically exploit technological vulnerabilities. Preventive measures, newsroom security practices and clear channels of cooperation with responsible institutions are therefore necessary.

In the long term, resilience is inseparable from education. Media literacy should be integrated into education programmes as early as possible, systematically developing skills of critical evaluation, source verification, argumentation and digital security. It is also important to create attractive and accessible tools to counter disinformation: interactive instruments, clear methodologies, and practical instructions tailored to different audiences, including older people and ethnic communities. Such tools work when they are not only "correct" and "factual" but also actually used.

The legal–regulatory dimension remains important, but must be continuously adapted to the realities of new media. Social networks and platforms have changed the logic of content distribution, requiring solutions that address disinformation and incitement to hatred more effectively while upholding democratic freedom of expression. In practice, this involves not only the letter of the law but also clear enforcement mechanisms, institutional capacities and cooperation with international platforms.

Resilience requires continuous expert dialogue and international cooperation. Regular forums, discussions and conferences strengthen shared situational understanding among policymakers, institutions, academia and journalists, enabling the exchange of experience and methodologies. International inter-institutional and non-governmental organisation cooperation remains necessary because authoritarian influence operations are transnational, and their neutralisation must be collective.

A separate but related point concerns international communication. The visibility of democratic narratives and reliable information in the international space – particularly in English – is an important response to disinformation aimed at global audiences. Strengthening strategic communication capacities in English and supporting such media content and projects contributes to the broader visibility of democratic positions and reduces the risk of informational vacuums that malicious actors often exploit.

Finally, particular emphasis should also be placed on the role of intelligence and law enforcement institutions in adapting to the new generation of Russian kinetic and diversionary operations. The Lithuanian case demonstrates that the transition from information operations to the planning of physical attacks, sabotage and terrorist acts requires not only political or communicative responses but also structural strengthening of security-sector capacities. This includes sustained investment in intelligence

and criminal-intelligence technologies, analytical capabilities, inter-institutional data sharing and specialist training able to identify the hybrid linkage between informational, logistical and kinetic activities. Such capacities enable the detection of hostile actors' operational footprints at an early stage, tracing transnational networks and disrupting operations before they escalate into overt violence. In the long term, this becomes a necessary condition for halting the evolution of the Russian strategy in the Baltic region from informational pressure towards deniable physical action, while strengthening the democratic state's ability to operate across both low- and high-intensity hybrid threat environments.

References

Bērziņa, I., Cepurītis, M., Kaljula, D., & Juurvee, I. (2018). Russia's footprint in the Nordic-Baltic information environment 2016/2017. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/russias-footprint-in-the-nordic-baltic-information-environment-20162017/138 Cepurītis, M., et al. (2020). Russia's footprint in the Nordic-Baltic information environment: Report 2019/2020. NATO Strategic Communications Centre of Excellence.

Galeotti, M. (2020, July 24). The UK must urgently adapt to Russia's "dark power" tactics. University College London. https://www.ucl.ac.uk/news/2020/jul/opinion-uk-must-urgently-adapt-russias-dark-power-tactics

Hobbs, R., & McGee, S. (2014). Teaching about propaganda: An examination of the historical roots of media literacy. Journal of Media Literacy Education, 6(2). https://doi.org/10.23860/jmle-6-2-5

Lietuvos nacionalinis radijas ir televizija. (2025a). Tarptautinis tyrimas: Slaptas Rusijos karas prieš Europą. https://www.lrt.lt/naujienos/lrt-tyrimai/5/2509172/tarptautinis-tyrimas-slaptas-rusijos-karas-pries-europa

Lietuvos nacionalinis radijas ir televizija. (2025b). Tyrimas: Vilnius tapo Rusų tarnybų paskirstymo centru – sprogmenys keliavo sekso žaisluose. https://www.lrt.lt/naujienos/lrt-tyrimai/5/2681906/tyrimas-vilnius-tapo-rusu-tarnybu-paskirstymo-centru-sprogmenys-keliavo-sekso-zaisluose

Lietuvos nacionalinis radijas ir televizija. (2025c). Teismas už partizanų vado paminklo išniekinimą trims užsieniečiams skyrė laisvės atėmimą. https://www.lrt.lt/naujienos/lietuvoje/2/2784105/teismas-uz-partizanu-vado-paminklo-isniekinima-trims-uzsienieciams-skyre-laisves-atemima

Maliukevičius, N. (2025). Fortifying democracies: Lithuania's comprehensive approach to counter disinformation and propaganda. Eastern Europe Studies Centre. https://www.gssc.lt/wp-content/uploads/2024/04/v05_Maliukevicius_Fortifying-Democracies_EN_A4.pdf

Prosecutor General's Office of the Republic of Lithuania. (2026). Criminal case concerning terrorist attacks in Šiauliai referred to court. https://prokuraturos.lt/lt/baudziamoji-byla-del-teroro-ispuoliu-siauliuose-perduota-teismui-with-text-in-english/11996

Riessman, C. K. (2005). Narrative analysis. In Narrative, memory & everyday life (pp. 1–7). University of Huddersfield.

Rizgelienė, I., Zubaitienė, V., Maliukevičius, N., et al. (2026). HALT-PROP: Human-annotated Lithuanian textual corpus for propaganda narratives and techniques. Scientific Data, 13, Article 47. https://doi.org/10.1038/s41597-025-06367-w

State Security Department of Lithuania. (2023). National threat assessment 2023. https://www.vsd.lt/wp-content/uploads/2023/03/ENG-2023-Gresmes-ENG-el_-1.pdf

State Security Department of Lithuania. (2024). National threat assessment 2024. https://www.vsd.lt/wp-content/uploads/2025/03/2024-03-07-VGV-EN.pdf

State Security Department of Lithuania. (2025). National threat assessment 2025. https://www.vsd.lt/en/reports/national-threat-assessment-2025/ Walker, C., & Ludwig, J. (2017). From soft power to sharp power: Rising authoritarian influence in the democratic world. National Endowment for Democracy. https://www.ned.org/wp-content/uploads/2017/12/Sharp-Power-RisingAuthoritarian-Influence-Full-Report.pdf

Zubaitienė, V., Maliukevičius, N., & Rizgelienė, I. (2025). Lingvistinės strategijos propagandiniuose tekstuose: Tekstynu grįsta diskurso analizė. Lietuvių Kalba, 20, 96–119. https://doi.org/10.15388/LK.2025.7

Malign Information Influence in Latvia 2020–2025: Unchanged Goals yet Evolving Playbooks

Dr. Una Aleksandra Bērziņa-Čerenkova

Director of the Latvian Institute of International Affairs

Introduction: Notes from the Hybrid Battlespace

The concept of *malign information influence (MII)* has evolved beyond traditional propaganda, disinformation or cyber interference. Today, it encompasses the **strategic orchestration of narratives, networks and legitimacy claims** designed to weaken democratic resolve over time. To refer specifically to MII conducted by foreign powers, the European External Action Service has introduced the concept of Foreign Information Manipulation and Interference (FIMI).[1] It is important to note that the FIMI approach sidesteps the problem of judging content on the true–false spectrum (the so-called "ministry of truth dilemma") by concentrating on the techniques, tactics and procedures (TTPs) of dissemination. This paper adopts the FIMI approach and therefore does not analyse the accuracy of narratives, but rather dives into the activities of the three main state actors that the Latvian State Security Service identifies as challenging Latvian information security: Russia, Belarus and China.[2]

Latvia has been consistently named as among the better-prepared European Union (EU) countries in countering disinformation[3] and, along with other Baltic states, even called "inspirational" in this regard.[4] Both the high level of attention and the creative response toolkit employed by Latvia are consequential: the Latvian information environment functions as a hybrid battlespace, as the nation has been at the centre of the overlap of authoritarian information influence approaches for years. Such perception is based not just on the realities faced on the ground but also on the operational conceptualisation of the perpetrators. Previous research into the role of information manipulation in the military doctrines of Russia and China has demonstrated that both treat psychological and cognitive domains as key battlegrounds. They also stress the importance of operating within an adversary's territory and have announced plans to run information operations within Western countries, directly targeting their populations.[5]

Russia's goal is to sow confusion and polarisation and to undermine societal resilience, ultimately eroding the structure of Latvian statehood. Belarus' goal, in addition to supporting Russia's, is also driven by strategic jealousy; therefore, it is largely domestic and aimed at countering Latvian soft power and the appreciation in Belarus of Latvia's path of development. China's goal is to improve its national image and regional standing through targeted engagement with opinion leaders, including those on the non-mainstream spectrum, and through dispersing stories of its development and grandeur.

As for TTPs, Russia continues to run **high-volume, disruptive operations** aimed at delegitimising democratic institutions, undermining NATO, harnessing existing fissures and eroding public trust through persistent, increasingly artificial intelligence (AI)-powered information manipulation. This prioritises receptivity among Latvia's Russian-speaking population, but also banks on the polarisation of the Latvian-speaking population along political and values lines. Belarus' approach is similar to Russia's, but lacks some of its capabilities. In contrast, China pursues a **low-volume, self-centred elite-driven strategy** that shapes narratives around global legitimacy, economic interdependence and "win–win" multilateralism, while engaging in information suppression.

All three actors exploit open societies, media fragmentation and algorithmic amplification. The dispersed narratives of Russia/Belarus and China overlap to some extent, but their objectives are only partially aligned; intensity and engagement results are also dissimilar. Against this backdrop, Latvia's experience provides an instructive case on **how to sustain democratic confidence in the face of sustained pressure from Russia and Belarus, as well as emerging pressure from China.**

Nothing New: On the Forefront of Russian Malign Information Influence

Russia's goals vis-à-vis the Latvian information environment have remained relatively unchanged in the past decade, with the exception of the intensification of Ukraine-related narratives since Russia's full-scale invasion of Ukraine in 2022. It seeks to divide the transatlantic community, undermine Latvia's societal resilience by amplifying sensitive issues, discredit Ukraine, target Latvian officials and institutions and pave the way to restore Russia's international standing.[6]

While Russia targets the transatlantic community in general, there are several factors that mean Latvia, in particular, plays a **symbolic and practical role** for such operations from Russia. First, Latvia's geopolitical position is one of bordering Russia and hosting key NATO forces. Second, the history of being part of the Russian Empire from 1721 to 1917, followed by the history of the Soviet occupation (1940/1944–1991), has socialised Latvians into contextualising, recognising and reacting to cultural and behavioural prompts that are viewed as "Russian", including language, popular culture, classical culture, media and humour. More than 90% of Latvia's inhabitants aged 35 years or older who do not speak Russian at home still report being able to communicate in Russian.[7]

Third, as a result of both of these historic periods, Latvia is home to a sizeable Russophone community: 34.6% of the population speaks Russian at home.[8] As Māris Andžāns argues, it is "important to note that neither of the groups, be it Latvian-speakers...or Russian-speakers, is homogeneous and static in their perceptions. The diverging perceptions are...underpinned by different and often polarising historical memories, and the stratification of the information space which is further reinforced by Russia's compatriot policy."[9] Previous research has shown that the language spoken at home is a statistically significant factor in narrative perceptions in the country, surpassing such factors as ethnicity, locality, religion and age.[10]

Since the 2022 ban in Latvia of all Russia-based media channels following Russia's full-scale invasion of Ukraine,[11] Latvia's Russian-speaking citizens increasingly consume hybrid information, including global YouTube channels, local Russian-language portals, Telegram news aggregators, WhatsApp interest groups and EU-based Russian-language media. Research by the Baltic Centre for Media Excellence[12] shows that while direct consumption of Russian state TV has decreased sharply since 2022, algorithmic feeds still **recommend Kremlin-aligned** humour or cultural **content** through online entertainment channels, adapted as both long-watch video essays and snippet-style vertical Tik-Toks or Threads. This maintains a **passive exposure loop**, reinforcing shareable, relatable, identity-based narratives without overt propaganda.

There is an opinion among Russian speakers that "the media cannot be independent at all".[13] This cynicism is also a result of the Russian propaganda approach, the so-called "firehose of falsehood". According to RAND, the main characteristics of Russian propaganda are that it is "rapid, continuous, and repetitive, and it lacks commitment to consistency",[14] which in turn obliterates the belief that truth exists and can be known. However, what is sometimes under-stressed is that this approach is, first, historical, and, second, domestic just as it is external. As Mark Jaryc observed in 1933, "Different both in structure and in objectives from any kind of Western journalism, the Soviet Press is, without doubt, one of the most interesting and significant features of New Russia".[15] Within the Russian linguistic space, the popular Soviet press, since its emergence, has been perceived, and rightly so, as a propaganda instrument of the Communist Party and thus the state, rather than a source of information, objectivity and, to put it bluntly, truth.

Today, as well, similar to the 1930s, rather than being an isolated weapon that is exclusively pointed towards outside audiences, the "firehose of falsehood" is an intrinsic characteristic of the information environment in Russia as a whole, and the perception that there can be no independent media and that everybody lies authentically transfers from the Russian domestic space into Russophone communities abroad. When Russian officials deny their responsibility, as in the case of the downing of flight MH17,[16] and shift the responsibility for war crimes to the Ukrainian side,[17] the information consumer walks away not necessarily with a belief in the Russian version, but often with a perception that the truth is unfindable in its nature and that the reality is much more complex than one can ever know. For example, a 2025 study, "Geopolitical perceptions, civic participation and media use of the Russophone population of Latvia", found that 89.3% of respondents agreed with the statement "today we are surrounded by so many different opinions and so much information that it is difficult to say what is true".[18]

The Latvian State Security Service points out that Russia's activities aimed at influencing information combine traditional broadcast media with digital platforms such as Telegram, TikTok, YouTube and various illicit distributors of Russian television content, with approximately 16% of Russian speakers maintaining access to banned channels via virtual private networks (VPNs).[19] These activities focus heavily on war propaganda and are particularly targeted at the populations in border regions, where analogue broadcasts remain accessible. Russian state media, political talk shows and entertainment content are disseminated alongside tailored messages produced by

pro-Kremlin activists who have relocated to Russia, while intelligence and security services exploit Telegram to conduct influence campaigns, collect information and even to cross the line into physical action and solicit attacks on Latvian soil.[20] Coordinated operations by troll networks and fake accounts on TikTok and Facebook amplify socially sensitive topics, spread hostile narratives about Ukraine and NATO, and attempt to erode trust in Latvian officials, institutions and the democratic process as a whole. Russia seeks to present culture, entertainment and sport as domains detached from politics, thus tapping into its cultural and historical recognisability, while, of course, these spheres are integrated into its influence toolkit.

The Service underscores that Russia's information operations are closely aligned with its foreign policy goals, aiming to fragment the transatlantic community, weaken Western societal cohesion, delegitimise Ukraine's statehood and destabilise Latvia's internal environment by provoking divisions, amplifying discontent and sustaining narratives favourable to Moscow. An EU DisinfoLab factsheet identifies several narratives that are spread by Russia's FIMI efforts in Latvia[21]:

- Revival of Nazism;
- Latvia and the West are preparing for war with Russia;
- Latvia violates the rights of non-citizens;
- Latvia is a failed state;
- Latvia was better off in the USSR.

The Grass is Greener on the Eastern Side of the Border: Malign Information Influence from Belarus

While Belarus is not a top-tier player in global information influence activities, the Latvian State Security Service still considers it to be among the most visible FIMI actors in Latvia.[22] The goal of Belarus is twofold: to amplify Russian messaging and to counter Latvia's soft power and the appreciation of Latvia's path to development domestically. Belarus uses the resources of its media, including BelTA and Nexta, as well as the official accounts of state institutions, e.g. the State Border Committee of Belarus, both directly through their respective online presences and through secondary dissemination of their content through reposts via other social media accounts, including YouTube, Facebook, TikTok and Telegram.

The material is geared towards eliciting an emotional response, including interviews with people and families who have relocated to Belarus, people presented as refugees assaulted by Latvian border guards, and video reports demonstrating a supposedly lower quality of life in Latvia than in Belarus. On top of the overarching amplification of official Russian views on Ukraine, there are several more specific narratives emanating from Belarus aimed at demonising Latvia among Belarusians and assuring them of the superiority of Lukashenka's regime, which nonetheless spread to the Latvian online information space:

- the Latvian state is infringing on the rights of its Russian-speaking population;
- the Latvian state is infringing on the values of its traditional-leaning population;[23]
- Latvian border guards are cruel to migrants;[24]
- Belarus and its regime provide a great future for people fleeing Latvia; [25]
- Latvia is a failed state.[26]

A Recent and Self-Consumed Scene: China as a Malign Information Influence Actor

Although the People's Republic of China (PRC) is a relative newcomer to the Latvian information space, it has nonetheless been named as a FIMI actor in the country. Currently, Latvia is a secondary recipient of the PRC's narratives, which are primarily geared towards the West in general and Europe in particular. This signifies a change in the PRC's approach, as prior to the early 2020s, Latvia, like other nations that China viewed as "Central and Eastern European", was a recipient of a hybrid PRC discourse. The messages included narratives vis-à-vis the West, as well as narratives of "socialist friendship"[27] and even South–South frames, such as offers of cooperation, including PRC loans and infrastructure.[28]

However, since the early 2020s, the PRC's approach to information disseminated in the Baltic region, including in Latvia, has shifted. The socialist friendship story has been dropped (not least due to its total lack of impact in a country that had been occupied by a Communist power rather than having undergone a homegrown socialist experiment), and the South–South proposals have taken a backseat, as there was never any demand for PRC loans due to the availability of EU funds and frequent incompatibility in legislature.

Instead, narratives around economic cooperation, as well as the PRC's global standing, have moved to the fore. Interestingly, even though the greatest challenge facing Latvia–China relations is China's tacit support for Russia's invasion of Ukraine, PRC information activities do not

seem to actively counter this reputational damage. This may be a testament to the relative immaturity of China's cognitive operations in catering to local contexts.

Although not at the centre of the PRC's information manipulation strategy, Latvia remains a target due to historical factors and current developments. First, Latvia has a history of official engagement with Taiwan. China believes that Latvia came close to recognising Taiwan diplomatically during the period when consular relations were in place between 1992 and 1994.[29] Therefore, the Baltics in general (due to the fact that neighbouring Lithuania became an advocate for exchanges with Taiwan post-2021[30]) and Latvia in particular can act in direct opposition to the PRC's core interests.

Second, Latvia's NATO membership makes it a strategically relevant target for PRC information manipulation, because both the NATO alliance as a whole and the US in particular increasingly frame China as a systemic challenge and a pacing threat. By shaping narratives in NATO member states, including Latvia, the PRC seeks to weaken NATO cohesion and reduce support for policies that constrain China. Therefore, influence efforts in Latvia could allow Beijing to exploit societal divisions, thereby undermining political consensus on Euro–Atlantic security issues.

Third, Latvia is an EU member state, which makes it part of the political, regulatory and normative structures that Beijing seeks to influence. For Beijing, cultivating a more favourable informational environment in smaller EU member states offers a cost-effective way to soften EU-wide criticism, reduce cohesion on China-related policies and promote frames that legitimise China's global role while discouraging alignment with transatlantic approaches that Beijing views as constraining its strategic objectives.[31]

What characterises PRC information influence attempts in Latvia is that China mainly speaks about itself. The PRC does not comment on Latvian politics, except for debates related to its core interests. China's stories are a part of China's global communication efforts. In contrast to other Nordic–Baltic countries, such as Sweden, the narratives of China in Latvian media are not derived from locally adapted content but rather appear through translations of China's global communication channels, such as China Central Television (CCTV) or Xinhua News Agency.[32]

There is, however, another side to the PRC's approach to the Latvian information space: malign influence through information suppression. Information suppression is defined as a "set of actions to silence information with the purpose of muting dissenting voices or narratives within and outside a country's borders, serving the interest of strengthening a regime's grip on power",[33] and therefore forms part of the FIMI toolkit. Cases of information suppression are difficult to map as they often remain unreported, and definitively pinpointing an event on the spectrum of outside pressure vs. self-censorship is challenging. However, several events indicate that information suppression is present as a PRC influence tactic in Latvia.

In 2024, the University of Latvia reportedly accepted, but then moved to exclude, presentations at the Baltic Alliance for Asian Studies conference that included discussions on topics such as Hong Kong, Taiwan and Tibet. This led to accusations of academic censorship and influence exerted by China.[34] That same year, the PRC Embassy exerted pressure on the Dailes Theatre to cancel a performance by the Shen Yun troupe, which is part of the Falun Gong religious organisation that is banned in the PRC.[35]

To spread its narratives in the Latvian information space, Beijing relies on:

- **Official diplomacy and earned media** - op-eds written by ambassadors, interviews and public-relations placements in mainstream outlets;
- **Academic partnerships** and think-tank cooperation, subtly guiding research agendas through funding or access incentives;
- Selective use of social media (e.g. Facebook, X, LinkedIn) to echo official statements rather than drive mass engagement.[36]

The narratives the PRC is spreading through the channels identified above include:

- China provides business opportunities for local entrepreneurs;[37]
- China appreciates Latvia;[38]
- China is a leader in addressing climate change;[39]
- China is the guardian of multipolarity and the UN.[40]

Rising Up to the Challenge: Latvia's Defences in the Information Space

While Latvia's resilience architecture, including media literacy, fact-checking, cybersecurity and legal solutions, is among the most developed in the EU, vulnerabilities remain. Audiences continue to be exposed to Russian cross-border information attacks, not least along linguistic lines; Belarus targets Latvia both out of support for Russia and strategic jealousy; and China engages in positive spin publicly while privately attempting information suppression. In the long term, chronic exposure to hybrid threats risks public fatigue.

To counter these challenges, various national policies have been introduced.

The Latvian National Concept on Strategic Communication and Security of the Information Space (2023-2027)[41] established a proactive framework designed to transition the state from a reactive posture to systemic defence. The policy prioritises the "whole-of-society" resilience model, integrates high-level strategic coordination across government branches with grassroots media literacy initiatives, and supports independent local journalism. The framework follows the TTP mindset, proposing measures such as the institutionalisation of early-warning monitoring systems to detect FIMI, the implementation of rapid-response protocols for crisis communication, and closer cooperation with NATO and EU partners.

The Cybersecurity Strategy of Latvia 2023-2026[42] also contains provisions on information security, as it merges the policy and operational expertise of the Ministry of Defence and CERT.LV (the Cyber Incident Response Institution of Latvia) into a unified National Cyber Security Centre to strengthen critical infrastructure and increase protection against the technical disruptions that often accompany disinformation campaigns.

Finally, the 2024 amendment to Latvia's Criminal Law introduced criminal liability for influencing the electoral process via deepfake technology. Latvia's criminal code now prescribes severe penalties for the malicious use of deepfake technology during election cycles, i.e. during the 120-day pre-election window and on the day of the vote itself. Specifically, the law criminalises the intentional creation or dissemination of fabricated, defamatory content targeting political parties or candidates for the national parliament, local councils or the European Parliament, with offenders facing community service, probation or short-term detention, with the most serious violations carrying a prison sentence of up to five years.[43]

Together, these documents aim to create a comprehensive strategic and legal framework that comprises both soft and hard measures.

Conclusions and Recommendations: From Threat Awareness to Strategic Confidence

Latvia's information space has long been a testing ground for authoritarian experimentation. However, it is equally a proving ground for **European resilience**. The experience of countering corrosive cynicism from Russia and Belarus and resisting China's disciplined narrative management offers a broader lesson: **small states can innovate** in counter-influence policy when they anchor trust at the local level and coordinate regionally.

Based on the insights presented in this paper, several recommendations are offered for the Latvian and, indeed, the wider European approach to countering information manipulation.

1) Less content verification, more TTP-based monitoring: The L**atvian National Concept on Strategic Communication and Security of the Information Space (2023-2027) sets out a framework for a FIMI approach in Latvia. If it is to work**, Latvian intelligence and media oversight bodies should divert resources to identifying how information is being disseminated (e.g. AI-powered amplification, coordinated troll networks), not simply fact-checking what is being said. This will enable the neutralisation of botnets and illicit distributors while sidestepping "true–false" or freedom-of-speech debates.

2) Combat cynicism through transparency: To counter the pervasive belief, including among Russophone populations, that "the truth is unfindable", official communication should prioritise building trust by admitting it if information is unavailable or if mistakes are made. Policies should support independent investigative journalism, not least by ensuring the financial stability and resilience of the public broadcaster, LSM.

3) Protect academic freedom: Establish a formal reporting mechanism and legal protection framework for academic and cultural institutions facing pressure from foreign embassies. Policy should explicitly prohibit excluding academic topics based on foreign intervention, ensuring that institutional funding is not contingent on self-censorship to appease foreign state actors.

4) Invest in much more of the same: Latvia should continue to professionalise its information-resilience ecosystem through both soft measures, such as civic education and predictable communication, and hard measures, including the expansion and strict enforcement of the legal toolkit.

Along with its closest neighbours, Latvia is, as the saying goes, "building the plane while flying it", i.e. not only developing but also immediately applying approaches to protect its information space. With partners in the Nordic–Baltic 8 and beyond, the nation can serve as a **model for an adaptive European democracy** capable of withstanding and outlasting chronic coercion.

References

1 https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

2 https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf, p.42

3 https://www.euronews.com/my-europe/2025/01/07/which-european-countries-were-most-exposed-to-disinformation-last-year-radio-schuman

4 https://www.hybridcoe.fi/wp-content/uploads/2025/10/Hybrid_CoE_Research_Report_15_Countering_disinformation_Euro_Atlantic.pdf, p.45

5 https://deconspirator.eu/wp-content/uploads/2025/10/WM_D2_3.pdf, p.44

6 https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf, p.45

7 https://stat.gov.lv/lv/statistikas-temas/izglitiba-kultura-zinatne/izglitibas-limenis/publikacijas-un-infografikas/21018?themeCode=IZ

8 https://data.stat.gov.lv/pxweb/en/OSP_OD/OSP_OD__apsekojumi__pieaug_izgl/PIA77.px/table/tableViewLayout1/

9 Māris Andžāns, Multi-ethnic societies and willingness to defend one's own country: Russian-speakers in the Baltic states, Lithuanian Annual Strategic Review 19(2022), no. 1, 47-68, DOI 10.47459/lasr.2021.19.3

10 https://www.gssc.lt/wp-content/uploads/2024/02/Classic-Cleavages-in-a-New-Light.pdf

11 https://eng.lsm.lv/article/features/media-literacy/all-russia-based-tv-channels-banned-in-latvia.a460236/

12 Presentation available at: https://bcme.eu/en/research/changes-in-media-consumption-russian-speaking-audiences-in-estonia-and-latvia/

13 https://bcme.eu/en/research/changes-in-media-consumption-russian-speaking-audiences-in-estonia-and-latvia/

14 https://www.rand.org/pubs/perspectives/PE198.html

15 https://www.jstor.org/stable/4202815

16 https://www.bbc.com/news/articles/cd62v890l5qo

17 https://www.dw.com/ru/loz-v-promyslennyh-masstabah-kak-rf-atakuet-es-dezinformaciej/a-64635535

18 https://science.rsu.lv/ws/portalfiles/portal/103500745/Latvijas_rusofono_iedz_vot_ju_eopolitiskie_priek_stati_pilsonisk_l_dzdal_ba_un_mediju_lieto_ana.pdf

19 https://science.rsu.lv/ws/portalfiles/portal/103500745/Latvijas_rusofono_iedz_vot_ju_eopolitiskie_priek_stati_pilsonisk_l_dzdal_ba_un_mediju_lieto_ana.pdf

20 https://www.iem.gov.lv/lv/jaunums/vdd-krievijas-specdienesti-aizvien-biezak-latvijas-valstspiederigos-kaitniecisku-darbibu-veiksanai-verve-telegram

21 https://www.disinfo.eu/wp-content/uploads/2025/08/20250809_Disinfo-landscape-in-Latvia-v2.pdf

22 https://vdd.gov.lv/uploads/materials/40/en/annual-report-2024.pdf, p.45

23 https://www.lsm.lv/raksts/zinas/medijpratiba/25.10.2025-baltkrievijas-medijs-nexta-izplata-kremla-propagandas-video-par-latviju-am-ludz-to-dzest.a619834/

24 E.g. see: "Ужасы на границе! Латвийские силовики избили беженцев до потери сознания!" https://www.youtube.com/watch?v=6pRLh___y6k ; "Избитых кубинцев обнаружили на границе с Латвией" https://www.facebook.com/watch/?v=1205198108166171

25 E.g. see: "Наконец-то сбежал из этого рейха!" // Блогер из Латвии переехал в Беларусь: ЧЕСТНЫЙ РАССКАЗ" https://www.youtube.com/watch?v=n2mWInkNyNU

26 E.g. see: "Четверть латышей живёт не в Латвии!" // Жизнь в Беларуси и Прибалтике: откуда бегут? "" https://youtube.com/shorts/g9kVz3wMJsk?si=adQbNihvsepScY4C

27 https://link.springer.com/epdf/10.1007/s10308-019-00550-6?author_access_token=OYMOmvWCncuJbhjhcen0Afe4RwlQNchN-Byi7wbcMAY5YGpCBDKQoEr8zVHjIUXf-RA3k9dRyAGTX2SQJF_jnvZsxP8o-OgnPdS4836VGy0rrlrfNHoI0y5Dk3Ep1Tz-9FVLcCLFSnw-jyL-Bu46bRfA%3D%3D&fbclid=IwAR24TY_9GSZttMT2QmC_AtSiXxrGYpC24JgDHRuWyjswWhpszXYHRYUlR84

28 https://mzv.gov.cz/file/862793/china_cee_cooperation.pdf

29 https://www.liia.lv/en/publications/not-important-enough-to-neglect-taiwan-in-the-diplomacy-of-northern-and-central-europe-1429?get_file=1, p.106

30 https://www.liia.lv/en/publications/not-important-enough-to-neglect-taiwan-in-the-diplomacy-of-northern-and-central-europe-1429?get_file=1, p.127-142

31 More on the PRC motivations and tools in EU, read: https://merics.org/sites/default/files/2020-04/GPPi_MERICS_Authoritarian_Advance_2018_1.pdf

32 https://stratcomcoe.org/pdfjs/?file=/publications/download/Chinas-Influence-in-the-Nordic-Baltic-Info-Environment-UPDATED.pdf?zoom=page-fit, p.87

33 https://www.arm-project.eu/wp-content/uploads/2024/08/ARM-Policy-Brief-01.pdf

34 https://www.lsm.lv/raksts/zinas/latvija/17.05.2024-bazas-par-akademisko-cenzuru-augstskolas-atsaka-dalibu-azijas-studiju-konference-latvijas-universitate.a554477/

35 https://www.delfi.lv/kultura/32026447/culturenvironment/120054286/kinas-vestnieciba-izdarijusi-spiedienu-uz-dailes-teatra-vadibu-zagars-dusmigs-vesta-tv3

36 https://stratcomcoe.org/pdfjs/?file=/publications/download/Chinas-Influence-in-the-Nordic-Baltic-Info-Environment-UPDATED.pdf?zoom=page-fit, p.43

37 https://nra.lv/pasaule/506576-mudina-latvijas-uznemejus-izmantot-kinas-ekonomikas-iespejas.htm

38 https://stratcomcoe.org/pdfjs/?file=/publications/download/Chinas-Influence-in-the-Nordic-Baltic-Info-Environment-UPDATED.pdf?zoom=page-fit, p.43

39 <iframe src="https://www.facebook.com/plugins/post.php?href=https%3A%2F%2Fwww.facebook.com%2FEmbassyofChinainLatvia%2Fposts%2Fpfbid0aKpBX1eghMuK4snzdeLorvGYu3sJXo8mFCR1BvZtwX7U2VsMgapPuQS6aGKzT2gHl&show_text=true&width=500" width="500" height="734" style="border:none;overflow:hidden" scrolling="no" frameborder="0" allowfullscreen="true" allow="autoplay; clipboard-write; encrypted-media; picture-in-picture; web-share"></iframe>

40 https://nra.lv/viedokli/kinas-tautas-republikas-vestnieks-latvija-tangs-songgens/495534-ano-statutu-atkartota-caurskatisana-labakas-nakotnes-varda.htm

41 https://www.mk.gov.lv/en/media/15446/download?attachment

42 https://www.mod.gov.lv/sites/mod/files/document/Kiberdrosibas%20strategija%202023%20ENG.pdf

43 https://lvportals.lv/skaidrojumi/363728-ievies-kriminalatbildibu-par-velesanu-procesa-ietekmesanu-izmantojot-dzilviltojuma-tehnologiju-2024

Mapping Russian Disinformation in Estonia

Marek Kohv

Head of Security & Resilience Programme at the International Centre for Defence and Security

Introduction

Estonia's information environment has become more vulnerable over the past decade, as Russian influence operations—following restrictions on Kremlin-controlled information channels—have shifted increasingly to social media, with growing use of deepfakes and artificial intelligence combined with algorithmic targeting. As a result, it has become ever more difficult for information consumers to distinguish authentic content from manipulated material and to verify the origin of the information presented.[1]

National threat assessments consistently place influence operations within the broader framework of hybrid threats, in which information influence supports efforts to shape foreign, security, economic, and energy policy.[2]

Such activity is more effective during crises and periods of social tension. This article examines Russian disinformation in Estonia primarily as a system of interconnected channels and dissemination infrastructure, rather than as a sequence of individual false claims. From the perspective of policy recommendations and countermeasures, what matters more is how influence operations are structured and function (i.e., through which channels and infrastructure they spread, and how they intervene in the public information space).[3]

In Estonian debates, there is often a tendency to focus on communication platforms and channels. Yet, the division of roles among the actors is at least equally important: who creates the content, who amplifies it, who confers legitimacy on it, who ensures its dissemination, and when this network is activated. The European Union's foreign information manipulation and interference (FIMI) approach similarly emphasises that it is not sufficient to focus only on false claims and misleading narratives; attention must also be paid to manipulative, intentional, and coordinated behaviour and—particularly in the context of the third FIMI threat report—to mapping the digital infrastructure used by foreign states.[4]

The NATO Strategic Communications Centre of Excellence's (NATO StratCom COE) Nordic–Baltic Eight (NB8) overviews also emphasise that the success of Russian influence operations always depends on the local context (historical divisions, linguistic space, institutional trust, and the media landscape), and therefore, the methods used must be linked to both the actors carrying them out and the target audiences.[5]

Objectives

Russian disinformation in Estonia is generally not aimed at refuting individual factual claims, but rather at shaping the political and social environment in ways that generate decision-making paralysis, declining trust, and persistent polarisation. This approach means that success is not necessarily measured by whether a specific false claim endures, but by whether public debate becomes more confused, more tense, and less effective, and whether people begin to doubt the competence and goodwill of institutions, the media, and allies.

In practice, this means that information influence is not a side effect but a supporting mechanism that can help prepare more favourable conditions for cyberattacks, economic coercive measures, or attempts to inflame social tensions, while at the same time making the state's response appear more contradictory and complex in the eyes of the public.

One of the central objectives is to erode trust in institutions and alliances (e.g., NATO, the European Union), because persistent doubt over "who is telling the truth" makes policy implementation and crisis management more costly and increases the likelihood of confrontation.

Trust is not always undermined through direct attacks; more often, it is weakened through small but repeated doubts—suggesting that decisions are being made "in someone else's interests," that the state is not in control of the situation, or that the presence of allies brings danger rather than security. In this way, a gradual situation emerges in which even well-founded decisions begin to appear

controversial to part of the audience—not because of their substance, but because of alleged hidden motives. As a result, explanations provided by politicians, officials, and experts lose credibility precisely because they are interpreted as the rhetoric of a particular faction. One example is the increase in defence spending. Even when higher defence expenditures are strategically justified, part of the audience may come to interpret official explanations primarily as a justification for tax policy. In this way, the crisis of trust shifts from substance (the need for defence capability) to motive (at whose expense and in whose interests).

A second example is education reform, which, according to the Ministry of Education and Research of Estonia, aims to ensure more equal and higher-quality education, improve Estonian language proficiency, strengthen social cohesion, and reduce segregation. Yet part of the audience may interpret it primarily as a security and integration policy measure. By contrast, another part may view it as identity-based pressure and the marginalisation of the Russian-speaking community.

Comparisons across the NB8 countries show that the openness of democratic societies and the plurality of opinions can become vulnerabilities when trust is systematically undermined, especially if public debate grows hostile and trust in institutions declines. When discussion becomes persistently suspicious and dismissive, the willingness to listen to differing views also decreases, and the public sphere begins to reward exposure rather than explanation—thereby creating fertile ground for subsequent influence operations.

A second objective is to divide society, which in Estonia often relates to tensions around linguistic space, identity, and historical memory. The core logic here is that polarisation does not need to create a single pro-Russian group; it is sufficient if different groups begin to perceive one another not as political opponents, but as morally suspect or hostile communities.

Under such conditions of antagonism, compromise becomes more difficult, because compromise itself comes to be seen as weakness or betrayal, and solidarity in times of crisis—whether a security, public health, or economic crisis—becomes more fragile. This logic of division does not require a unified Kremlin-aligned bloc to emerge; it is enough that distrust grows between different groups and that the willingness to reach agreements and engage in collective efforts declines, especially in situations where tensions are already high.

The ultimate goal is to create a situation in which society responds more slowly and more inconsistently to new crises, because attention and energy are consumed by internal disputes and the search for culprits rather than by solving problems.

Third, a further objective is to weaken the legitimacy of support for Ukraine and of sanctions policy by exploiting war fatigue and highlighting economic hardship.

This is often done in a way that does not directly attack Ukraine but instead shifts the focus to "our" suffering: rising prices, insecurity, fear of escalation, and the sense that the burden is not being shared fairly. Once this framing has been entrenched, it becomes politically more difficult to sustain long-term aid and sanctions policy. Public support begins to erode not primarily because of the substance of the arguments, but because of fatigue, frustration, and a sense of hopelessness.

Assessments by the Estonian Foreign Intelligence Service (Välisluureamet, EFIS) emphasise that such attitudes are strategically valuable to Russia, since they reduce long-term policy consistency and decisiveness in target states. In other words, even if no single narrative remains permanently dominant, it is already beneficial for Russia if policy becomes more erratic, decision-making slower, and collective action among allies more contested.

A separate objective is the delegitimisation of Estonian decisions, in which attention is shifted from the substance of a decision to suspicion about its intent (e.g., "externally directed," a "platform for provocation," or a "Russophobic project"). The central technique of delegitimisation is to make a decision appear suspicious first and in need of explanation afterwards. Therefore, institutions have to spend increasing amounts of time and trust capital not on justifying the decision itself, but on defending their own legitimacy.

This is especially effective when delegitimisation is linked to the previously described erosion of trust and social division: one part of society quickly adopts the suspicion, another reacts sharply against it, and the result is once again polarisation that reduces the space for substantive debate. The NB8 perspective shows that the same basic framing ("the West is to blame" or "escalation is inevitable") can be rapidly repackaged depending on whether the focus is security, the economy, or identity.

It is precisely this flexibility that makes delegitimisation so dangerous: the narrative does not need to remain strictly identical; it only needs to fit the prevailing emotions and the day's political issue, so that doubt and fatigue remain a persistent background condition.

Practices

In Estonia, Russian influence practices are most clearly

manifested as recurring operational mechanisms that bind narrative and dissemination into a single whole, and operate with varying intensity during different crises. Opportunities for influence operations emerge when public attention is already high and people are looking for quick explanations: crises, elections, remembrance days, security incidents, and economic shocks all provide fertile ground. That is because uncertainty increases the persuasive power of simplified and emotional interpretations.

The national risk assessment definitively links this shift to the move towards social media. It further emphasises that algorithm-driven targeting and technological manipulation can increase the visibility and spread of emotional content, making public debate more erratic in substance and less receptive to fact-checking. In other words, influence operations may succeed not by proving anything, but by generating many confusing signals at once, thus pushing people to rely on their prior assumptions rather than on verifiable information.

One of the central practices is **narrative framing and repetition**: an event is placed within a predefined interpretive frame, and the same core message is repeated across different channels in different formats (news item, image, comment, video, etc.), creating the impression that it is a widely shared understanding.

The effect of framing lies not only in the message itself, but also in the way the frame makes certain questions seem automatically pointless or ridiculous, thereby narrowing debate and pushing alternative explanations into the background. Repetition, in turn, works through psychological familiarity: even if a person does not fully believe a claim, they may begin to feel that "there must be something to it," simply because they have encountered the same idea repeatedly and in multiple places.

Another common technique is **comparative distraction and moral equivalence**, often presented as pointing out the claimant's hypocrisy. The discussion quickly shifts away from the original issue toward other conflicts, historical cases, or peripheral examples, until the possibility of tracing back the original fact and assigning responsibility is lost. The result is cynicism ("there is no truth," "everyone lies anyway," etc.), which reduces willingness to act and reinforces decision paralysis: if nothing can be trusted, then no political choice appears reasonable or legitimate. From the perspective of influence operations, this mood is highly valuable because it does not require the complete success of any single narrative. It is enough if society begins to function in a state of persistent doubt and fatigue.

A third important practice is **source laundering**, that is, obscuring the origin of information. A manipulated claim moves from an anonymous or unclear starting point through intermediary nodes that add an appearance of credibility until it reaches community discussion without a verifiable original source.
Along this dissemination chain, the form of the content may change: the original claim is first presented as a question or hint, then as news, then as analysis, and finally as someone's personal experience—so that the impression of evidentiary weight grows even as actual verifiability declines. An Estonian example is a video circulated in spring 2025 that was given a misleading interpretation suggesting allies' alleged attack readiness from Estonia, even though verification showed the footage came from a public military parade in Tallinn. This illustrates how decontextualised visuals can be used as "evidence," seemingly relieving viewers of the need to verify the source and timeframe.

In such cases, the core of the influence lies in the fact that the viewer "sees it with their own eyes," but does not see what is most necessary to see: where and when it was filmed, and what the depicted event actually means.

The fourth practice relies on **emotions** (fear, anger, fatigue), which shorten verification and increase the urge to share quickly, especially under conditions of economic stress and crisis fatigue.

Emotional content does not need to be sophisticated; often, a simple opposition (e.g., us vs. them), a hint of injustice, or fear of escalation is enough to trigger rapid spread, creating the sense that the situation is out of control and that someone is hiding the truth. Another Estonian example is the pressure generated by influence attempts around the refugee issue, as described by the police, aimed at creating tensions between Ukrainian war refugees and local residents by exploiting perceptions of fairness and competition over resources and amplifying these dynamics in community groups.[6] The danger of this logic lies not only in individual hostile posts, but in the fact that emotion can reshape the norms of community discussion: once negativity becomes routine, it begins to influence the attitudes of even neutral individuals and reduces willingness to show solidarity.

The fifth practice is the apparent **borrowing of authority**: a narrative is given an impression of credibility and expertise (analysis, documents, expert, etc.), which reduces scepticism and helps normalise messages even when they merely repeat familiar propaganda frames. This technique works especially well in situations where the audience has little time or limited knowledge of the issue, because an expert-looking format substitutes for verifiable content, and people may prefer a confidently presented conclusion to uncertainty.

In addition, it helps create the perception that this is not influence activity at all, but simply an alternative viewpoint, which in turn makes it harder to respond and

increases the message's durability.

The sixth practice concerns **coordinated amplification**, which is expressed through recognisable patterns: the same message appears in many places within a short period of time, participants play different roles (e.g., posting, commenting, provoking debate), and the content moves from one environment to another.

The aim of such coordinated dissemination is not always to persuade, but to pressure the public sphere into reacting: if a topic is suddenly everywhere, someone must respond to it, which can in turn give the original message additional visibility—even when its argumentation is weak. Coordinated amplification is especially effective when combined with the above-listed techniques: a decontextualised visual (source laundering), an emotional frame (fear or anger), and an appearance of authority (analysis) together create a situation in which content spreads faster than it can be calmly and convincingly refuted.

Actors

Understanding these practices requires distinguishing the division of roles among the actors involved, because the same techniques produce different effects depending on who creates the content, who adapts it to (Estonian) conditions, and who gives it local credibility. Estonian threat assessments emphasise that Russia uses a diverse set of tools and intermediaries in influence operations, as well as a combination of overt and covert activities. For this reason, analysis should focus on the operational mechanisms that generate influence, rather than only on proving the origin of individual posts.

This approach helps avoid two extremes: on the one hand, the temptation to explain everything through a direct command chain; on the other hand, the temptation to treat all suspicious patterns as merely opinions, even though many campaigns operate precisely through intermediary links and role differentiation.

Broadly speaking, the actors can be divided into four groups: Russian state actors; intermediaries and proxy channels; local legitimisers and disseminators; and platform/community structures. This typology captures both strategic direction and the local actors through whom influence is exercised in Estonia. State actors usually define the themes, timing, and strategic emphasis, but in practice, they may not conduct the day-to-day dissemination themselves; instead, intermediary layers are used to create apparent distance and localise the message.

The EFIS's perspective describes the higher-level context: Russia links information operations to its foreign policy objectives, and target states are treated differently, which also helps explain why certain accusatory and blame-oriented frames remain persistent in Estonia and reappear across different events.

At the same time, Estonia's experience shows that the role of local disseminators and providers of legitimacy can sometimes be more decisive than the visibility of the original source. The Baltic Engagement Centre for Combating Information Disorders (BECID) Tallinn case-based analysis describes how a pro-Kremlin content producer operated openly for years, built a channel with a large following, and expanded its influence in part through filming and gaining visibility at local events. As a result, propagandistic content became, for part of the audience, something considered worthy of discussion and remained in the public sphere longer than the typical life cycle of individual false claims would normally allow.[7]

It is precisely here that the practical meaning of legitimisation becomes visible. Influence does not arise only from the fact that something is claimed, but from the fact that the messenger is present within our information environment and has access, contacts, and continuous visibility—factors that normalise their role and make their messages feel familiar to part of the audience.

A second Estonia-specific example of actors concerns state-directed media structures and the intermediaries clustered around them. The end of Sputnik's activities in Estonia in late 2019 and early 2020 (in connection with the sanctions regime) shows that official channels of influence can face legal and economic constraints within Estonia's legal environment. At the same time, however, pressure emerges within Russia's information space to portray this as a violation of freedom of speech, thereby shifting attention away from the substantive issue (sanctions) toward a moral framing (persecution).[8]

Subsequent proceedings and charges related to sanctions violations involving former Sputnik employees confirm that influence operations also have their own ecosystem (employment contracts, financing, legal structures, etc.), which can be addressed not only from a communications perspective but also from a law-enforcement perspective.

A third Estonian case that helps illuminate the division of roles among actors is the April 2007 riots in Tallinn (the so-called Bronze Night), in which the Estonian Internal Security Service (Kaitsepolitseiamet, KAPO) already at the time emphasised both the extensive and distorted coverage by foreign media and the broader dimension of influence activity. This was not merely spontaneous street politics, but an event in which the information space, mobilisation, and state interests became intertwined, and in which different participants played different roles (some created the frame and narrative, others amplified it, and still others mobilised people).[9] The same logic is visible in the influence activity behind the mobilisation at the time, as part of a broader pattern. Yet, the 2022 removal of the

Narva tank did not trigger a similar violent escalation, which points both to the changed context (i.e., Russia's full-scale war against Ukraine) and to a shift in the societal reception environment.[10]

An important element of countering disinformation is identifying its perpetrators. In this regard, it is more useful to prioritise pattern detection—that is, a model of coordination and function—rather than focusing on exposing the entire command chain, which public data often does not allow. The advantage of this model is that it is suitable both for prevention and for monitoring: if a recurring division of roles is visible (e.g., who creates, who adapts, who lends credibility, who amplifies), it becomes possible to respond early and in a targeted way, without waiting for the full command chain to be uncovered.

Responses

In Estonia, several responses to FIMI have proven effective, but they also reveal clear limits that should shape next steps. What has worked best is a whole-of-society 'friction and transparency' approach: sustained public threat reporting by security institutions (creating a regular, credible baseline for public awareness); targeted legal and regulatory action against Kremlin-aligned outlets subject to sanctions or assessed as posing a security risk; and rapid public messaging during high-attention moments to reduce uncertainty and prevent agenda capture.

In particular, Estonia has also strengthened local high-quality alternatives to the Kremlin-affiliated media outlets in the Russian-language information space—most visibly through public-service and domestic Russian-language journalism initiatives (including ETV+ TV channel and related services). It, together with cooperation with civil society and volunteer networks, helps reduce dependence on Kremlin-aligned sources in parts of the Russian-speaking audience. The impact is visible in surveys illustrating that the significance and trust of Kremlin channels among Russian speakers in Estonia have dropped sharply since restrictions were introduced in 2022.[11]

At the same time, Estonia's experience also demonstrates which measures have underperformed: purely reactive debunking is often too slow against high-volume, emotionally framed content, while interventions aimed at restricting individual channels are frequently offset as influence networks shift across platforms and rely on broader digital infrastructure. Closed or semi-closed communities in lightly moderated or encrypted environments remain particularly hard to reach with corrective information, especially where institutional trust is low—precisely the conditions that FIMI actors exploit by coordinating amplification across multiple platforms and infrastructures.

Conclusion

Russian disinformation in Estonia is best understood as an ecosystem in which strategic objectives are realised through recurring practices and a division of roles among actors, and whose effectiveness depends on vulnerabilities in the local context. Indicators of this ecosystem include, for example, the framing of decontextualised visuals (i.e., source laundering) and the creation of social antagonism through emotional tactics, both of which can be rapidly amplified in community networks.

People increasingly move across different linguistic spaces and the information channels of their own communities. As a result, different understandings emerge of what is true and how events should be interpreted, so that the same incident may signify one thing for one group and something entirely different for another. Recent integration and media studies in Estonia show that the war in Ukraine has altered media consumption among both Estonian- and Russian-speaking populations in several ways. It has brought part of the Russian-speaking population closer to Estonia's media space and led some residents to stop consuming Russian media, while alienating others.[12]

The danger lies not only in the spread of false claims but also in Russia's multi-layered information and influence activities. In Estonia, such activities aim to undermine trust and cooperation, deepen societal divisions, and constrain decision-making space through the imposition of Russia's will.[13]

Estonia's most effective response to FIMI has been a whole-of-society approach combining transparency, regulation, and credible alternatives. Regular threat reporting by security institutions, targeted legal action against sanctioned Kremlin-aligned outlets, and rapid public communication during sensitive moments help reduce uncertainty and limit narrative dominance. Strengthening Russian-language public-service media and domestic journalism has also reduced reliance on Kremlin information sources among parts of the Russian-speaking audience.

Notwithstanding successes, Estonia's experience also reveals clear limitations: reactive debunking is often too slow; single-platform interventions are easily bypassed; and closed or encrypted communities remain difficult to reach, particularly where trust in institutions is low.

References

1 Government Office Republic of Estonia (Riigikantselei), National Risk Assessment: Environment and Emerging Risks (chapter PDF) (Tallinn: Riigikantselei, n.d.), https://riigikantselei.ee/en/riskid/hostile-special-services#read-more.

2 Estonian Foreign Intelligence Service (Välisluureamet), International Security and Estonia 2026 (Tallinn: Välisluureamet, 2026), https://raport.valisluureamet.ee/2026/assets/VLA_ENG-raport_2026_WEB.pdf.

3 European External Action Service (EEAS), "3rd EEAS Report on Foreign Information Manipulation and Interference Threats," 19 March 2025, https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en

4 European External Action Service (EEAS), "Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)," https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

5 NATO StratCom COE, Russia's Information Influence Operations in the Nordic-Baltic Region.

6 ERR News, "Police in Estonia Fending Off Info Operations Targeting Ukrainians," September 20, 2022, https://news.err.ee/1608697378/police-in-estonia-fending-off-info-operations-targeting-ukrainians.

7 Baltic Engagement Centre for Information Disorders (BECID), HOT REPORT (December 2025) (Tartu: BECID, University of Tartu, 2025), https://becid.ut.ee/wp-content/uploads/2025/12/HOT-REPORT-December.pdf.

8 ERR News, "Former Sputnik Employee Charged with Breaking International Sanctions," May 14, 2024, https://news.err.ee/1609342116/former-sputnik-employee-charged-with-breaking-international-sanctions.

9 International Centre for Defence and Security (ICDS), "Russia's Involvement in the Tallinn Disturbances," May 11, 2007, https://icds.ee/en/russias-involvement-in-the-tallinn-disturbances/ ; Edward Lucas, "The Evolution of Russian Hybrid Warfare: Estonia," Center for European Policy Analysis (CEPA), January 29, 2021, https://cepa.org/article/the-evolution-of-russian-hybrid-warfare-estonia/.

10 For more on the case, see: Marek Kohv, "The Case of Estonia: Navigating Disinformation in the Shadow of Russian Influence," in ISDP Special Paper: Disinformation (Stockholm: Institute for Security and Development Policy, December 2024), https://www.isdp.eu/wp-content/uploads/2024/12/ISDP-Special-Paper-Disinformation.pdf

11 ERR News, "Survey: Kremlin Channels Lose Significance with Russian Speakers in Estonia," April 12, 2022, https://news.err.ee/1608562720/survey-kremlin-channels-lose-significance-with-russian-speakers-in-estonia.

12 NATO Strategic Communications Centre of Excellence (NATO StratCom COE), Russia's Information Influence Operations in the Nordic-Baltic Region (Riga: NATO StratCom COE, 2024), https://stratcomcoe.org/publications/russias-information-influence-operations-in-the-nordic-baltic-region/314.

13 Estonian Internal Security Service (KAPO), Annual Review 2024–2025 (Tallinn: Kaitsepolitseiamet, 2025), https://kapo.ee/sites/default/files/content_page_attachments/annual-review-2024-2025.pdf.

Russian Information Influence on Finland Before 2022 and Prospects Afterwards

Jussi Lassila

Senior Research Fellow at the Finnish Institute of International Affairs

Introduction

The overwhelming majority of Finns would agree that relations between Finland and Russia can be divided into two distinct periods: before and after February 2022. Russia's war of aggression in Ukraine led Finland, alongside Sweden, to join NATO – a development widely regarded as Russia's most significant foreign policy defeat resulting from its invasion. During the war, hostile influence operations directed at Finland have reached unprecedented levels, although Finland has been generally well-prepared to counter them. The greatest concern during the NATO accession process centred on the "grey zone" between submitting the application and receiving membership approval, when strong Russian countermeasures were feared. However, these did not materialise, largely due to Russia's glaring failure to achieve its initial objectives in Ukraine throughout 2022.

To date, the most serious of Russia's influence tactics against Finland following the decision to join NATO have been the instrumentalisation of migration at the Finnish–Russian border in 2023 (first time observed in 2015), along with repeated large-scale disruptions of air and maritime navigation systems – a "natural" consequence of Russia's efforts to shield strategic assets in its border regions from Ukrainian strikes. Finland has not yet experienced sabotage operations on its soil similar to those seen elsewhere in Europe,[1] although strong suspicions persist regarding Russian-backed proxy actors being behind recent damage to subsea infrastructure.[2]

Despite the radical deterioration in bilateral relations, Finland has avoided overly alarmist reactions to the Kremlin's behaviour, reflecting relatively robust preparedness against information influence. Fearmongering about Russia primarily serves Moscow's own objectives, as a key aim of its information warfare is to paralyse adversaries through fear.[3] For instance, exaggerated concerns about Russia's military readiness against NATO could erode political willingness to support Ukraine. Indirect information influence linked to sabotage fears surfaced in the summer of 2024 following a series of unexplained break-ins at water towers.[4] The clearest example of such indirect influence relates to the prolonged closure of Finland's eastern border since late 2023, which has sparked tensions and criticism among Russian-speaking residents who have been the Kremlin's main targets in the West.

To assess the potential of Russia's influence in the post-2022 context, this chapter examines Russia's information influence against Finland since the early 2000s and Finland's preparedness to counter this.

Overview of Russian Information Influence Against Finland and Conditions Surrounding it During the 2000s

Regarding Russia's information influence on Europe, Finland has been a particularly challenging target. This difficulty stems from a distinctive feature of Finnish domestic politics: unlike many European countries, Finland has maintained a strong consensus on foreign and security policy – particularly regarding Russia – despite the presence and even governmental participation of a major right-wing populist party. In other words, although the Finns Party shares nearly all of the core agendas of its populist counterparts in other European countries – such as opposition to immigration, conservative–nationalist values and criticism of climate policies – it does not share the pro-Kremlin sympathies common among many European populist parties.[5]

The same applies to Finland's far-left party, the Left Alliance, which throughout the 2010s positioned itself as a progressive, green–left opponent of Putin's Russia.[6] Particularly noteworthy is that, despite its historical roots as a successor to the Communist Party of Finland and its prior comprehensive NATO scepticism, the Left Alliance ultimately supported Finland's NATO membership in spring 2022, aligning with public opinion and parliamentary majorities.

Beyond this broad security-policy consensus, Finland has also been shielded by its relatively small and heterogeneous Russian-speaking minority, whose size and composition differ considerably from those in Estonia and Latvia. For Russia, leveraging compatriot policies and instrumentalising Russian-speaking minorities abroad has been a central priority.[7] This has also manifested in Finland.

In brief, compared with many European states lacking a similar consensus and hosting politically more influential, sizeable numbers of pro-Russian actors, Finland has been well-protected against Moscow's influence.[8] Finnish authorities also demonstrated vigilance against influence campaigns well before the annexation of Crimea. A notable case occurred in 2009, when Russia politicised child custody disputes in its media and sought to establish a bilateral child affairs commission – a proposal Finland rejected. Ultimately, Russia acceded to the Hague Convention on International Child Abduction, implemented between Finland and Russia in early 2013.[9]

Custody disputes marked the Kremlin's first visible influence campaign against Finland in the 2000s, exposing the limitations of Finnish officials' traditional confidentiality norms when such issues are politicised by foreign powers. Silence from Finnish authorities fuelled Russian propaganda, as the information vacuum was actively filled by Kremlin-friendly pseudo-experts such as Johan Bäckman.[10] However, these disputes sharpened Finland's strategic communication, and in 2012, the Kremlin-aligned Komsomolskaya Pravda published a comprehensive article based on official Finnish data, correcting earlier false claims.[11]

The Finnish authorities' readiness to counter disinformation was evident again in 2016, when decisive responses neutralised false and possibly coordinated claims in Russian- and English-language discussions about the Russian-language background of victims of a triple homicide in Imatra – a border town with a sizeable Russian-speaking minority.[12] Finally, in 2017, the European Centre of Excellence for Countering Hybrid Threats was established in Helsinki.

The gradual deterioration of Russia's previously positive image of Finland – from the early 2000s to the late 2010s – and its collapse following Russia's war of aggression reflects Moscow's authoritarian and revisionist trajectory. Given Russia's limited capacity for direct influence in Finland, its primary tool has been shaping Finland's image in Russian state-controlled media, which serves to justify Kremlin policies to domestic audiences. These efforts aim to recast Finland's image from "too positive" to one aligned with official narratives. Despite these attempts, annual surveys commissioned by Finland's Ministry for Foreign Affairs and conducted by the Levada Center since 2017 indicate that Finland's image has remained relatively neutral among Russians, particularly among younger cohorts.[13]

Of the Nordic countries, Finland received the most attention in Russian media between 2000 and 2024.[14] This pattern has remained largely stable, except in 2018, 2021 and 2023, when Sweden was mentioned more frequently. Interestingly, despite Sweden's smaller Russian-speaking minority compared with Finland, Russia was notably more active in targeting Russian speakers in Sweden with influence campaigns, for example, in 2016.[15]

Following the annexation of Crimea, Russian media narratives about Finland emphasised trade relations and sought to portray Finland as sympathetic to Russia. A striking example of manipulative reporting was a January 2015 article in Nezavisimaya Gazeta, claiming that "Finland's foreign minister sees no need to scare people with the Kremlin threat", and that "Estonia summoned Finland's ambassador over remarks opposing the creation of an EU-wide Russian-language 'counter-propaganda channel'".[16] In reality, then-Foreign Minister Erkki Tuomioja had criticised Baltic states in Finland's leading Swedish-language newspaper Hufvudstadsbladet for failing to address the need for Russian-language news for their minorities in response to Russian pressure, citing European Union (EU) proposals to counter Kremlin propaganda. Estonia's displeasure was genuine, but contrary to Nezavisimaya Gazeta's claim, Tuomioja advocated for Russian-language counter-propaganda, while accusing the Baltic states of nationalist language policies.

This case exemplifies Russian state media's systematic distortion of foreign statements to fit official narratives – portraying Finland as a friend of Russia, unlike "nationalist" Baltic states. The same template has been applied since Finland's decision to join NATO, with repeated claims that Finns oppose NATO but were coerced by Western powers (primarily the US) into a contrary policy.

From the perspective of Russia's domestic communication strategy, the key objective is to depict Western countries – even if they impose sanctions and are NATO members – as maintaining ties with Russia. Secondary news items are eagerly exploited, whether accurately or through distortion, to reinforce this narrative. A telling example came after the EU imposed sanctions for the invasion of Crimea: a report circulated by multiple regional editions of Komsomolskaya Pravda on 18 January 2015, quoting former Estonian Foreign Minister Urmas Paet as saying "Finns value relations with Russia more than joining NATO".[17]

These narratives align closely with a 2016–2017 analysis by NATO Strategic Communications Centre of Excellence (StratCom) of the five most common themes in Russian state media coverage of Finland:[18]

- Claims about refugees destabilising society;
- Finland and Russia are good partners despite tensions;
- Ridiculing the notion of a Russian threat;
- Sanctions harm the EU (including Nordic states) more than Russia;
- NATO as a threat to Russia.

Migration has been a central theme fuelling political polarisation in democracies throughout the 2000s. Particularly after the reputational damage caused by Crimea's annexation, Kremlin strategic messaging began exploiting European migration debates by presenting Russia as an attractive ideological and civilisational alternative – while avoiding overt racism.[19] In Finland, this has typically surfaced in certain alternative media outlets.

The Kremlin's ambition to challenge what it perceives as Western media hegemony fostered connections – albeit loose and often indirect – between Russian actors and Finnish alternative media established in the 2010s. Russian strategic narratives targeting foreign audiences resonated and were disseminated to Finnish readers via major international propaganda platforms such as RT and Sputnik, often without explicit attribution. Common themes included systemic failures of liberal democracy, border security, ethnic tensions and claims of EU and US power grabs at the expense of Finnish sovereignty.[20]

Finland's NATO membership did not significantly alter the qualitative nature of these narratives. Assertions that NATO membership undermines Finnish independence and reflects hostility toward Russia – while serving US and supranational interests – have circulated in these media outlets since Crimea's annexation.[21]

The influence of Finnish-language alternative media remains limited, but fragmentation of media consumption and growing societal polarisation create the potential for expansion. As in other European contexts, the COVID-19 pandemic was a critical moment, energising anti-vaccine and conspiracy-oriented communities whose narratives the Kremlin sought to amplify. In Finland, suspicions arose around the Koronarealistit ("Corona Realists") website, hosted on Russian servers in 2021.[22]

Russian propaganda exerts its strongest influence on Finland's Russian-speaking population. Consumption of Russian state media within diaspora communities remains one of the Kremlin's most effective soft-power tools. Many long-term residents continue to watch Russian state television and often echo Kremlin narratives. Media use is particularly pronounced among those with limited Finnish language skills and pro-Kremlin attitudes. Conversely, some linguistically integrated individuals deliberately combined "alternative" sources – including Russian-produced content – in an attempt to triangulate the truth.[23]

Unlike some European states, Finland has not banned Russian state television channels. Instead, its strategy has focused on providing credible Russian-language public information and promoting media literacy. While integration into Finland's high-trust media environment offers some protection, Kremlin-friendly messaging still permeates diaspora networks via online alternative media and social platforms. Russian-language social media and certain YouTube channels host Finland-focused groups where Kremlin narratives – such as claims of NATO aggression or Russia's "protection of compatriots" – are propagated. Measuring their impact is difficult, but Helsinki University's study Diasporas during conflict found that Russian speakers actively engaged with Finnish media and society expressed stronger support for Ukraine, whereas those who felt alienated or relied primarily on Russian media tended towards ambivalence or adopted Kremlin views.[24]

A persistent challenge has been the limited resources of Finnish-produced Russian-language media. The best-known outlet, Spektr, ceased operations in 2021 for financial reasons, and its successor, Finskaya Gazeta, began echoing Russian state propaganda.[25] Although Finland's public broadcaster YLE launched regular Russian-language news in 2013, these efforts alone cannot saturate the Russian-language media space in Finland. Financial vulnerability among commercial actors creates clear exposure to Russian economic incentives and influence.

Since the early 2010s, Russia has actively targeted Finnish organisations, promoting integration of Russian speakers, in line with its compatriot policy objectives; in some cases, it has succeeded. For example, in 2012, the entire leadership of FARO, a Finnish Russian-speaking association, was replaced by pro-Russian actors, shifting its focus from integration to promotion of Russian culture.

Russia's broader strategy of exploiting migration-related polarisation in Europe has also manifested among Russian speakers in Finland. Social media discussions and interviews frequently reveal negative attitudes towards immigration, particularly regarding the 2015 refugee influx. These views often mirror narratives prevalent in Russian state media, which actively stoke divisions over migration in Europe.[26] Such attitudes may partly reflect efforts to elevate social status in a context perceived as unequal – particularly in the labour market. Divergent media environments between country of origin and residence, combined with ongoing geopolitical conflict, further reinforce echo chambers, creating fertile ground for Russian influence.

Beyond Russian state media, the Russian Orthodox Church – particularly parishes under the Moscow Patriarchate – has served as an important channel of influence among Russian speakers in Finland. Some attend Moscow-affiliated churches rather than those under Finland's autonomous Orthodox Church, underscoring Moscow's reach. The war in Ukraine has also heightened sensitivities within Finland's Orthodox community, with some actors reportedly avoiding explicit condemnation of Russia's actions for fear of alienating Russian-background congregants.[27]

Efforts to politically mobilise Russian speakers in Finland have been limited, although attitudes differ from those of the majority population. A 2022 survey by the Cultura Foundation found that 64% of Russian speakers condemned Russia's invasion of Ukraine, 18% deemed Moscow's actions justified and the remainder were undecided or unwilling to state an opinion.[28] Notably, by 2025, trust in Finnish media among Russian speakers ranked among the lowest of all language groups: 54% expressed trust in YLE, compared with 82% among Finnish speakers.[29]

Openly pro-Kremlin activism has met resistance. For instance, an attempt by pro-Russian activists to organise a Victory Day car rally with Russian flags in Helsinki in 2022 failed due to a lack of support from both Finns and local Russians. Russia's ability to activate "professional compatriots" in Finland remains limited, and even older generations with Soviet-era ties generally reject overtly imperialist–nationalist gestures.[30] Even so, despite Finland's relatively low strategic weight and the challenges facing Russia's influence operations, attempts have been made and, in some cases, partial successes achieved.

After 2022: What Should Be Done?

The comprehensive hostility of Russia's influence operations towards Finland was expected following Finland's decision to join NATO. In particular, the accusations and smear campaigns directed at Finland in Russian media reflect the Kremlin's frustration and the limitations of its toolkit. Traditional and softer means of influence – economic relations and the associated political leverage – have been lost. Militarily, Finland has long been among the best-prepared states in Europe, even before NATO membership, and its ability to counter increased cyberattacks is strong.

Regarding Russia's cheapest method, information influence, Finland has been shielded by a broad security policy consensus. Russia's recurring efforts to tarnish Finland's World War 2 history with Soviet-era propaganda narratives, such as accusations of widespread Finnish fascism, particularly following Finland's NATO decision, have found virtually no resonance in Finland. The most significant potential threat lies in the erosion of national unity through societal and political polarisation.

In this respect, Finland's Russian-speaking population is on the front line, as Russia intensifies its influence efforts following the weakening of previous options. There are known cases where Russian state actors have monitored refugees and anti-war migrants who arrived in Finland following the invasion of Ukraine, collected information about them and sought to sow distrust. The aim is often to intimidate activists and prevent open resistance. The linguistic connection of Russian speakers and their many family ties to Russia constitute a significant vulnerability, which is further fuelled by prejudices and economic challenges in Finland, particularly in Eastern Finland. For example, the border closure, which has continued since late 2023, has provoked strong opposition among many Russian speakers in Finland and has given some Russian-speaking politicians in Eastern Finland political leverage.[31]

In this regard, Finland should consider the long-term appropriateness of certain security measures. For instance, among many Russian speakers who actively oppose Putin, there is widespread distrust regarding the rationale behind decisions made by Finnish immigration authorities. Eroding trust in Finnish society inevitably provides the Kremlin with a weapon for indirect influence if the decisions of Finnish authorities generate fear and suspicion among opponents of Putin's regime.

The distrust of Finnish institutions and the susceptibility of Russian speakers to Kremlin narratives should be taken much more seriously. The generally broad integration of Russian speakers into Finnish society should be utilised more effectively rather than resorting to simplistic and populist securitisation. This underscores the importance of social cohesion as Finland's most effective shield against hostile influence. The erosion of this cohesion, for example, through economic difficulties and their geographical concentration (particularly in Eastern Finland), may in the longer term generate demands for the restoration of "pragmatic" relations and trade with dictatorial Russia, as many populist movements in Europe have demonstrated.

References

1 Jones, S.G. (2025) Russia's Shadow War Against the West. CSIS (18 March 2025), https://www.csis.org/analysis/russias-shadow-war-against-west

2 In brief: Estonia-Finland cable disruption, ERR.EE (26 December 2024), https://news.err.ee/1609560782/in-brief-estonia-finland-cable-disruption

3 Snegovaya, M. (2015). Putin's Information Warfare in Ukraine. ISW, https://www.researchgate.net/publication/282326292_Putin's_Information_Warfare_in_Ukraine

4 Vesilaitosten murrot voivat olla Venäjän pelottelua, arvioivat asiantuntijat, YLE (2 July 2024), https://yle.fi/a/74-20097494

5 Fagerholm, A. (2024). Far left and far right party reactions to Russia's invasion of Ukraine. West European Politics.

6 Wondreys, J., March, L., & Pytlas, B. (2025). My enemy's enemy is my friend? European radical left parties' response to Russia's war in Ukraine, The British Journal of Politics and International Relations, 27(3), 696–719.

7 Russia's footprint in the Nordic – Baltic information environment, Report 2016/2017, NATO Stratcom of Excellence, https://stratcomcoe.org/pdfjs/?file=/publications/download/final_nb_report_14-03-2018.pdf?zoom=page-fit

8 Revealing Russian influence in Europe: Insights from Germany, France, Italy and Ukraine. Report by Institute of Innovative Governance Black Sea Trust Fund of the German Marshall Fund (January 22, 2024), https://www.gmfus.org/news/revealing-russian-influence-europe-insights-germany-france-italy-and-ukraine

9 Haagin lapsikaappaussopimusta aletaan soveltaa Suomen ja Venäjän välillä ensi vuoden alusta alkaen, Oikeusministeriö (26 October, 2012), https://oikeusministerio.fi/-/haagkonventionen-om-bortforanden-av-barn-borjar-tillampas-mellan-finland-och-ryssland-fran-och-med-ingangen-av-nasta-ar

10 Dosentti lietsoo Venäjällä epäluuloa lasten huostaanotoista Suomessa, YLE (15 October, 20212), https://yle.fi/a/20-102034

11 Rassledovanie KP: Pochemu Finlyandiya otbiraet detey u russkikh mam, Komsomol'skaya Pravda (23 October 2012).

12 Mantila, M. & Mölsä, J. (2024) Valehtelua, vakoilua ja valtiollista vaikuttamista. Informaatiovaikuttaminen aseena Suomessa, Venäjällä ja USA:ssa. Docendo.

13 Ulkoministeriön selvitys (2025): venäläisten suhtautuminen Suomeen kaksijakoista, nuorten asenteet myönteisimpiä, Ulkoministeriö 14.10.2025, https://um.fi/tiedotteet/-/asset_publisher/ued5t2wDmr1C/content/ulkoministerion-selvitys-venalaisten-suhtautuminen-suomeen-kaksijakoista-nuorten-asenteet-myonteisimpia/35732

14 Information retrieved from the Russian media's Integrum information search portal.

15 Russia's footprint in the Nordic 2016/2017. The proportion of Russian speakers in Sweden is approximately 0.2% of the population, and in Finland, approximately 1%.

16 MID Finlyandii: Pora prekratit' pugat' narod Kremlem i rossijskoj ugrozoj, Nezavisimaya gazeta 16.1.2015.

17 Eks-glava MID Estonii: Finny predpotštut otnošenija s Rossijej vstupleniju v NATO, Komsomol'skaja pravda 18.1.2015

18 Russia's footprint in the Nordic, s. 74

19 Braghiroli, S., & Makarychev, A. (2018). Redefining Europe: Russia and the 2015 Refugee Crisis. Geopolitics, 23(4), 823–848. https://doi.org/10.1080/14650045.2017.1389721

20 Oivo, Teemu (2026). Venäjän laaja-alainen vaikuttaminen Suomeen 2000-luvulla. VNTEAS-raportti (forthcoming).

21 Russia's Information Influence Operations in the Nordic - Baltic Region, NATO Stratcom report (25 November 2024), https://stratcomcoe.org/publications/russias-information-influence-operations-in-the-nordic-baltic-region/314

22 Oivo, Teemu (2026). Venäjän laaja-alainen vaikuttaminen.

23 Davydova-Minguet, O. & et al. (2016). Suomen venäjänkieliset mediankäyttäjinä. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 35/2016. https://julkaisut.valtioneuvosto.fi/items/c003de28-1ec2-4aff-8486-99badec3c4e0; Vihalemm, T. & Juzefovičs, J. (2022). How Baltic Russian-speaking audiences outmaneuver securitization, essentialization, and polarization in times of crisis? Journal of Baltic Studies, Vol. 53, 4.

24 Jasinskaya-Lahti & al. (2024). Diasporas during conflict: A mixed-method analysis of attitudes of the Russian-speaking community in Finland towards the Russia-Ukraine war. Journal of Community & Applied Social Psychology, 34(4); Zavadskaya, M. (2026). Venäjän laaja-alainen vaikuttaminen Suomeen 2000-luvulla. VNTEAS-raportti (forthcoming).

25 Salovaara, O. (2021). Venäjänkielinen Spektr sai uuden elämän Finskaja Gazetana. Journalisti. https://journalisti.fi/artikkelit/2021/03/venjnkielinen-spektr-sai-uuden-elmn-finskaja-gazetana-suomen-uusin-venjnkielinen-media-kiinnostaa-mys-venjn-valtiota/

26 Davydova-Minguet, O. & et al. (2016). Suomen venäjänkieliset mediankäyttäjinä.

27 Kiista Ukraina-rukouksesta teki särön ortodoksikirkon maineeseen, YLE (23 February 2025), https://yle.fi/a/74-20145289

28 Cultura Foundation (2022). Russian Speakers in Finland, https://cdn.sanity.io/files/b0z6puta/production/30cdd37219f3f054fc2fb8542301adf541dce7f0.pdf

29 Suomessa asuvat vieraskieliset luottavat Ylen uutisiin, mutta ovat huolissaan toimeentulostaan ja rasismista, YLE (28 October 2025), https://yle.fi/a/74-20189315

30 Pro-Russian convoy set to pass through Helsinki region this weekend. (4 May, 2022). YLE, https://yle.fi/a/3-12429390

31 Venäjä-mielisellä agendalla valtuustoon, Ilta-Sanomat (8 June, 2025), https://www.is.fi/kotimaa/art-2000011280116.html

Russian Influence Operations Towards Sweden

Martin Kragh

Deputy Centre Director of the Stockholm Centre for Eastern European Studies (SCEEUS) and Senior Research Fellow at the Swedish Institute of International Affairs

On 17 September 2022, the official Twitter (now X) account of the Russian Embassy in Sweden posted the following message: "This is how the USA planned the war and the energy crisis in Europe". The "war" was apparently a reference to Russia's invasion of Ukraine in February of the same year. The message was accompanied by a link to an article published by Nya Dagbladet, a Swedish-language website associated with the far-right party Nationaldemokraterna (the "National Democrats"). Within a short time, their story had been picked up by several Russian media outlets, including RT, Rossiiskogo Gazeta and Tsargrad, a website affiliated with Russian media mogul and self-described pro-monarchist Konstantin Malofeev.[1]

The original story, published by Nya Dagbladet, alleged a US conspiracy to weaken the European economy through the promotion of war with Russia. According to a "leaked document" from the RAND Corporation, a US security policy think tank, such a scenario would shatter German sovereignty, perceived as a threat to US interests, and undermine any strengthening of relations between Russia and Europe. Furthermore, a collapse of the European economy would create such unfavourable socioeconomic conditions on the continent that "USD 7–9 trillion" would inevitably flow to the US, an outcome the document describes as "a controlled crisis".

The RAND document was revealed to be a fake. However, it is a reminder of how influence operations can be ambiguous and difficult to attribute to a particular state or non-state actor. In this case, what is known is that a fake story was published by an obscure Swedish-language website and amplified by a social media account formally subordinated to the Russian Ministry of Affairs. Subsequently, it was disseminated by several Russian-language media outlets. As a result, a recognisable pattern could be discerned: a Russian influence operation originating in a forgery with murky origins.

A Snapshot of Recent History

The purpose of influence operations is to shape public opinion and decision-making among a target audience, thereby creating conditions more favourable to the sender. In addition to a short-lived Sputnik Swedish-language website in 2015–16, there have been several different Russian influence operations towards Sweden in recent years, including propaganda and disinformation campaigns, the spread of forgeries, and various cyberattacks. A network of "Pravda" websites, published in a variety of languages, including Swedish, has also become operational.[2] In conjunction with these efforts, Russian politicians and diplomats have been active in attempting to shape Swedish domestic political affairs, particularly regarding NATO and Baltic Sea security. Other prevalent themes have been Swedish–Ukrainian relations, issues related to crime and alleged Swedish support of terrorism.

Forgeries

Forgeries have been a recurring element of Russian influence campaigns. In most instances, they originated in a similar fashion, usually through an obscure Russian- and/or Swedish-language website or blog. Some forgeries have utilised fake letterheads and purported to be written by Swedish decision-makers, presumably to gain credibility and an aura of authenticity.

A contextual analysis of how forgeries have been planted and distributed reveals linkages to Russian-sponsored originators. These linkages may be direct or indirect, but typically follow a similar pattern. Forgeries and accompanying explanatory "news articles" usually appear for the first time on websites such as cont.ws and politrussia.com (Russian-language websites), then in (poor) Swedish translation on Pressbladet, and later on websites in different languages (such as indymedia.org.uk, cyberguerilla.org and CNN's Ireport, where in the past, forgeries in many languages were regularly uploaded). The websites used have shared the common feature of allowing users to self-publish content.

It is reasonable to treat this series of forgeries and fake news items as an element of a single, consistent influence campaign. In 2015–16, around 25 forgeries were planted in the Swedish information space. An analysis

conducted by a team of researchers in 2020 identified the campaign against Sweden as part of a broader effort by a Russian state actor to sow political divisions in Europe and within NATO.[3] They concluded that there was little evidence of this particular campaign being effective, and that the main themes in the campaigns targeting Sweden were NATO cooperation and support for Ukraine.

Forgeries involving Swedish politicians and decision-makers focus on similar narratives, i.e. conspiracies involving Ukraine, terrorist organisations and NATO. A notable example is the case of a video, published on social media in September 2024 and amplified by Russian TV host Vladimir Soloviev, purporting to show how a Russian military attack that led to the death of several Swedish "military instructors" in Poltava. It was also suggested that the incident had forced Tobias Billström to resign as a Minister of Foreign Affairs, although no evidence for this claim was ever presented.[4]

Election Interference

In 2018, Russian propaganda outlets RT and Sputnik International made a concerted effort to emphasise and amplify the problems – alleged and real – related to crime and migration in Sweden. It was, to a large extent, in conjunction with these campaigns that Sweden became a disproportionate priority in Russian international propaganda outlets (relative to other Nordic–Baltic countries). Simultaneously, several peculiar forgeries appeared, perhaps reflecting a botched campaign to smear the Swedish parliamentary election that was also conducted in 2018. The forgeries were designed to smear the Sweden Democrats, Sweden's most well-known anti-immigration party, as insufficiently patriotic.

One notable forgery was a letter purporting to be from the US Secretary of State at the time, Mike Pompeo, to his Polish colleague Jacek Czaputowicz.[5] The letter claimed that the US had learned about the deep ties between the Sweden Democrats and Russian security services. The goal of Russia, Pompeo alleged in the letter, was to control the Sweden Democrats to further its interests in Sweden and the European Union (EU). A second forgery was a letter claimed to be from Marine Le Pen, the President of France's Rassemblement National, to Jimmie Åkesson, the leader of the Sweden Democrats. In this letter, Le Pen promised to provide 127 election observers and organisational support for the Sweden Democrats in the Swedish election.[6] Lastly, a third forgery was a letter purportedly written by Ukraine's former Prime Minister Volodymyr Groysman to his Minister of Information Policy, Yuriy Stets. In this letter, Groysman revealed a far-reaching Ukrainian conspiracy to interfere with the Swedish elections to advance the agenda of the Social Democrats and the Green Party, and to damage the Sweden Democrats.[7]

Hack-and-Leak Operations

There have also been cases of so-called "hack-and-leak" operations. In 2017 and 2018, Sweden's Sports Confederation was the victim of a cyberattack later attributed to "Fancy Bear", a group within Russia's military intelligence, the GRU.[8] In spring 2017, following an ISIS terrorist attack in central Stockholm, an alleged screenshot from a conversation between the terrorist and his handler appeared on the Russian propaganda website www.politonline.ru, one day after the event. Referencing a Twitter account created to vaguely resemble a collaboration between the Russian independent TV station Dozhd and the Kavkaz Center, but with an alleged sympathy for Islamist jihad (https://twitter.com/tvjihad), the article provided previously unknown information about the terrorist and his organisational ties to a terrorist cell in Dagestan.[9] A technical analysis of the terrorist's mobile phone later confirmed that the conversation was indeed authentic, although it remains unclear how the screenshot first appeared on a Russian-language website.

Sweden's Application for NATO Membership

Russian media reporting describing Swedish society as inherently anti-Russian intensified following Sweden's formal application for NATO membership in 2022. One example of this was in the run-up to Russia's full-scale invasion of Ukraine, when the Russian ambassador to Sweden made a statement about the increasing Russophobia in Sweden.[10] Russian politicians and pundits also heavily criticised Sweden's decision to apply for NATO membership.[11] Then, in spring 2024, an anonymous group of people threw manure over the fence of the Swedish embassy in Moscow.

Russian media and political leaders also amplified the problems that arose following a series of Quran burnings in Sweden by an Iraqi asylum seeker and a Swedish–Danish far-right activist. "Did they not have enough by Peter the Great?", quipped Vladimir Putin, using the burnings to deflect attention from an anti-Jewish pogrom in Dagestan.[12] Similar Quran burnings in Russia have also been blamed on people receiving "inspiration" from Sweden, including at the United Nations, where Sweden, Denmark and the Netherlands were accused by Russia of fomenting a "war" against religion. Lastly, in 2023, the Quran burnings were tied to Sweden's application for NATO membership. An activist allegedly burning the NATO statutes – a minor incident that went unnoticed by the Swedish media – was used as a pretext to claim that "they" (i.e. the Swedes) did not in fact want to join NATO.[13]

Lastly, it is worth noting a change in Russian narratives targeting Sweden in relation to the full-scale invasion of Ukraine in February 2022. Prior to the invasion, the main narratives depicted Sweden as a country witnessing societal collapse due to non-European immigration[14] and moral decay.[15] After the invasion in 2022, most of the narratives were related to Sweden's potential membership of NATO and support for Ukraine. For example, the narratives stated that Sweden was a vassal state that was being used by the US and NATO,[16] that membership of the alliance would be detrimental to the Swedish economy, and that it would lead to a weakened security situation for Sweden and the entire Baltic Sea region.[17] Following the formalisation of Sweden's NATO application later in 2022, Russian actors began to focus more on depicting Sweden as an unreliable NATO ally and a state that was weak and a hub for terrorism.[18] After Sweden's membership of NATO was finalised in March 2024, there was a notable decline in reporting related to Sweden's membership of NATO; subsequently, the narratives that were prevalent prior to Russia's invasion of Ukraine have increased once more.

Concluding Discussion

There is strong continuity in Russia's foreign policy goals towards Sweden. Since the early days of the Cold War, maintaining Sweden's military non-alignment was a key strategic interest. The largest information influence operation conducted by Russia towards Sweden in recent years was also connected to the question of Swedish–NATO cooperation. The Swedish government's application to join NATO in spring 2022, followed by formal membership on 7 March 2024, can be regarded as a clear Russian strategic failure. In this regard, Russian information influence operations have proven ineffectual and potentially counter-productive, as they contributed to raising public awareness in Sweden regarding Russian foreign policy conduct.

However, Russian setbacks in the military or diplomatic arena are no reason for complacency. The continuation of military hostilities in the Russo–Ukrainian War and the subsequent increase in tensions in the Baltic Sea region suggest that Sweden could again be the target of Russian influence activities in the future. Their relatively low cost, combined with plausible deniability, makes influence activities an attractive option. The historical fault line in Swedish domestic politics regarding NATO could be one potential vector of attack. Other societal fault lines, such as the issue of problems connected to crime and/or migration in Sweden, have already been favourite targets of Russian state media and could also be so in the future. Notably, domestic and foreign policy dimensions can overlap, as in the case of Quran burnings, and anti-Swedish protests in the Middle East. Another area that Russia may have an incentive to target is foreign policy, such as military support for Ukraine or sanctions on Russia. Often, the exact origin of a campaign is difficult to determine with certainty.

In assessing the potential effect of Russian influence operations, it is important to remember that they can also be amplified for three different target groups: a Russian domestic audience, a Swedish domestic audience and/or an international audience. Therefore, any response to Russian influence activities must be sufficiently flexible to reach not only a Swedish audience but also audiences in other geographical areas, depending on the character of the particular campaign. The attacks against Swedish diplomatic missions in the Middle East, following the news about Quran burnings in Sweden, are a case in point. Campaigns can erupt quickly and with little forewarning. In such instances, it is crucial that various societal actors – from the government level to media, academia and civil society – have the tools necessary to manage and/or comprehend a potential threat.

In response to growing threats from state-sponsored disinformation and foreign interference campaigns, successive Swedish governments have taken certain steps to strengthen societal resilience and protect critical institutions. First, the Psychological Defence Agency (MPF) was established in 2022 and formally tasked by the government to identify and counter foreign malign information influences. The agency serves as a central coordinating body across government departments to detect and analyse disinformation campaigns targeting Swedish society. Second, the establishment of a national elections protection network brought together the Swedish Security Service, the Psychological Defence Agency, the National Cybersecurity Centre and other agencies to provide political parties with awareness-raising support in how to identify and counter foreign malign information influence during elections. Third, media and information literacy (MIL) has been integrated into the educational system. Educational interventions have become central to building long-term societal resilience against disinformation. Fourth, international cooperation through multilateral networks has been strengthened, including a Memorandum of Understanding with the US, collaboration with Nordic neighbours and the EU, and observation status in the G7 Rapid Response Mechanism. This external dimension recognises that counter-influence efforts require coordination across borders.

Sweden's approach to combating foreign interference relies heavily on a whole-of-society strategy, learning lessons from other elections that have been targeted, and employing digital literacy campaigns and trusted civil society organisations as crucial elements of an effective response to Russian disinformation. For example, thou-

sands of civil servants have been trained to spot foreign influence campaigns, and similar training has been conducted for political parties and journalists.

Sweden's experience demonstrates that a coordinated, whole-of-society approach combining institutional mechanisms, public education, international cooperation and civil society engagement can effectively counter foreign influence operations. However, the persistence of threats and the emergence of new challenges indicate that this effort must be sustained and continuously refined to remain effective against an adaptable adversary.

References

1 https://x.com/RusEmbSwe/status/1571044179467464706 https://nyadagbladet.se/utrikes/chockerande-dokumentet-sa-plane-rade-usa-kriget-och-energikrisen-i-europa/ https://tsargrad.tv/articles/informacionnaja-bomba-zapadnyh-smi-raskryt-zakazchik-jenergokrizisa-i-vojny-na-ukraine_628180

2 https://sweden.news-pravda.com/world/2025/11/12/20744.html

3 https://secondaryinfektion.org/report/executive-summary/

4 <https://www.svt.se/nyheter/utrikes/falsk-text-om-doda-svenskar-i-poltava-spreds-i-ryska-medier>; <https://omni.se/billstroms-avgang-anvands-i-ryska-propagandakanaler-kopplas-till-attack-i-poltava/a/nyGbvB>.

5 https://postimg.cc/VJm9MjzD

6 https://postimg.cc/RWWKx9Lx

7 https://www.thestudentroom.co.uk/showthread.php?t=5554230

8 https://www.reuters.com/article/idUSKBN2C01V5/

9 https://www.politonline.ru/interpretation/22889936.html#

10 Russian embassy in Stockholm Facebook. 19 January, 19 2022: https://archive.is/YGUvz

11 https://www.theguardian.com/world/2022/jun/29/russia-condemns-nato-invitation-finland-sweden

12 Full statement available here: <https://tass.com/politics/1640391>, accessed on 18 April, 2024.

13 See <https://www.rbc.ru/rbcfreenews/64af16069a79478558477fd8>, accessed on 18 April, 2014.

14 Language Barriers Endanger Elderly Swedes' Lives – Report, Sputnik, 13 June 2018, accessed on July 4, 2024 https://sputnikglobe.com/20180613/sweden-elderly-care-migrants-1065359375.html

15 'Russia-Friendly' Swedish Right-Winger Backs Down Amid Smear Campaign, Sputnik, 23 October 2018, https://sputnikglobe.com/20181023/sweden-democrats-russia-1069131660.html Главком армии Швеции возглавил парад однополых извращенцев (ФОТО), Tsargrad.Tv, 4 August, 2019, accessed on 4 July, 2024. https://tsargrad.tv/news/shvedy-i-finny-poterjali-sovest-dengi-a-teper-i-son-govorit-budut-russkie-rakety_968669 <https://https://tsargrad.tv/news/shvedy-i-finny-poterjali-sovest-dengi-a-teper-i-son-govorit-budut-russkie-rakety_968669

16 Военный эксперт объяснил нежелание Швеции размещать базы НАТО, Izvestya, 12 March, 2024, https://iz.ru/1663787/2024-03-12/voennyi-ekspert-obiasnil-nezhelanie-shvetcii-razmeshchat-bazy-nato, Accessed on 10 July, 2024.

17 Шведы и финны потеряли совесть, деньги, а теперь и сон. Говорить будут русские ракеты, tsargrad.tv, 4 march, 2024, accessed on 4 july, 2024. https://tsargrad.tv/news/shvedy-i-finny-poterjali-sovest-dengi-a-teper-i-son-govorit-budut-russkie-rakety_968669 <https://https://tsargrad.tv/news/shvedy-i-finny-poterjali-sovest-dengi-a-teper-i-son-govorit-budut-russkie-rakety_968669

18 Украина через посольства за рубежом вербует наемников для ВСУ, RIA Novosti, 7 April, 2024, Accessed on 4 July, 2024. https://ria.ru/20240325/ukraina-1935664843.html

Russian Disinformation in Denmark

Jeanette Serritzlev

Military Analyst and Senior Advisor at the Royal Danish Defence College

Introduction

"President Volodymyr Zelensky is willing to send Ukrainian soldiers to Greenland, if the US invades" and *"European countries plan an assassination attack on the American president with help from Ukrainian special services"* (The Insider, u.å.). Such stories circulated online in January 2026 amid the tense situation between the US and the Kingdom of Denmark, sparked by the American president's statements about Greenland. These are, of course, fake stories and part of a Russian disinformation campaign labelled Matryoshka (Møller, 2026a), most likely with the aim of creating division and sowing distrust *in* and *about* Denmark and Ukraine. These are just some of the many different Russian attempts to target European countries, including Denmark, with a broad range of hybrid attacks, including in the cognitive domain.

This article provides a brief introduction to Danish society, followed by an assessment of the two main issues regarding current Russian disinformation threats in Denmark. The second half of the article describes the Danish approach to countering disinformation and offers recommendations to improve the country's resilience.

As a Nordic country, Denmark is traditionally a high-trust society, with a public education system that emphasises media literacy. Both societal factors are typically considered important parts of a cognitively resilient society. The current centrist coalition government (as of January 2026) is composed of three parties: one left-leaning, one centrist and one right-leaning. Denmark is also a country with a strong economy, a low unemployment rate and a welfare system that protects those outside of the job market. Compared with many other European countries, Denmark is a relatively homogeneous country (Ministry of Foreign Affairs of Denmark, u.å.-b) with a high degree of equality (Ministry of Foreign Affairs of Denmark, u.å.-a). Denmark held the highest ranking in Transparency International's Corruption Perceptions Index in 2024 (Transparency International, 2025), and Reporters Without Borders' Freedom of the Press Index ranked Denmark sixth in 2025 (Reporters Without Borders, u.å.).

Assessing the threat from Russian disinformation and other influence activities, the Danish intelligence services have consistently concluded that Denmark is not a prioritised target. Clearly, as a small state, Denmark does not hold the same strategic interest as larger countries such as France or Germany. However, Denmark is, in fact, present in Russia's disinformation and propaganda map (Libetrau & Tetzlaff, 2025, s. 100). This was also acknowledged by the head of counterintelligence of the Danish Security and Intelligence Service, Anders Henriksen, in a press release following the European Parliament elections in June 2024. Anders Henriksen confirmed that *"[w]e are constantly seeing Russian attempts to influence the Danish population"*, i.e. not only with regards to the European Parliament elections (Danish Security and Intelligence Service, 2024).

An interesting point about the disinformation threat is the fact that there seems to be a tendency for it to be more about Denmark, in order to shape perceptions of the country abroad, rather than directly influencing a Danish national audience (NATO Strategic Communications Centre of Excellence, 2024, s. 16; Rosengren, 2024). This will be explored more in the following section.

Main Narratives

This article considers the two main topics of disinformation in and about Denmark to be Ukraine and Greenland, the latter following the renewed interest, including direct threats, from the US president.

Ukraine

Since Russia's full-scale invasion of Ukraine in February 2022, Denmark has been a firm supporter of Ukraine and a strong voice in the European Union (EU) for supporting Ukraine and invoking sanctions on Russia. This Danish support for Ukraine is consensus-based across parliament and is also reflected among the Danish population.

Today, after nearly four years of Russian aggression, almost half of Danes support Denmark's contribution to Ukraine. In a survey conducted in December 2025, 49%

considered that the support was sufficient, 6% that it was too low and 31% that it was too high (Klærke, 2025). Even though this shows a high degree of support, the survey was reported in the Danish media as indicating a shift away from the unconditional support seen since 2022. Anti-Ukrainian disinformation has, in general, had a limited impact in the Danish information space. However, the change in attitude and the potential greater division in views are risks that could be used by actors engaging in Russian or pro-Russian disinformation. A prominent Danish professor of Political Science from the University of Aarhus described in an interview how he now saw *"clear signs that criticism of support for Ukraine has become a completely legitimate point of view in the public debate"* (Christensen, 2025), unlike earlier during Russia's war in Ukraine.

Greenland, the Kingdom of Denmark and the United States

The US president's aspiration of "acquiring" Greenland is not new. Neither is disinformation related to this issue. It appeared in 2019, 2025 and 2026. In both 2019 and 2025, alleged Russian disinformation used the division with pretty simple, but highly effective means in forms of forged products: Respectfully a letter in 2019, a social media post in 2025. In 2026, this has evolved into fake media stories.

In 2019, shortly before a planned state visit to Denmark, the US president first raised the idea of "buying Greenland". This was followed by a clear rejection from the Danish Prime Minister, Mette Frederiksen, calling it *"an absurd discussion",* which resulted in the cancellation of the state visit by the US president (NATO Strategic Communications Centre of Excellence, 2024, s. 26).

Not long after the visit was cancelled, a forged letter appeared online and reached the Danish media. The letter was attributed to Ane Lone Bagger, Greenland's then foreign minister. The letter was addressed to the US senator Tom Cotton, who, according to his own statements, was the person who inspired President Trump to discuss buying Greenland (NATO Strategic Communications Centre of Excellence, 2024, s. 26–27). The letter has since been described by the Danish Security and Intelligence Service as "highly likely" made and distributed by Russian influence actors to *"create confusion and possible conflict in the relationship between Denmark, the USA and Greenland."* (Danish Security and Intelligence Service, 2022, s. 18).

Since the re-election of Donald Trump in the 2024 presidential election, Trump's view on Greenland has reappeared as a political issue, not only in Greenland and Denmark but also within the EU and NATO member states. Even before taking office in 2025, Donald Trump threatened at a press conference that he would *"tariff Denmark at a very high level"* if the country resisted his territorial ambitions. On the same occasion, he also stated that he would not rule out using American military force to retake control of the Panama Canal, and also to seize Greenland (Gedeon, 2025).

The Danish Defence Intelligence Service (DDIS) produces an annual public threat assessment, Intelligence Outlook. In 2024, DDIS wrote: *"Denmark, the Faroe Islands and Greenland are not a specific priority target for Russian influence campaigns. However, Russia will likely also include Denmark, the Faroe Islands and Greenland in its influence campaigns targeting the EU, NATO or the wider Western world."* (Danish Defence Intelligence Service, 2024, s. 28).

Shortly afterwards, that assessment proved to be correct. A picture of a fake post on X started circulating more widely on social media. The post claimed to be from the Danish Member of Parliament Karsten Honge, stating that *"[i]n a situation of extreme escalation and tension, we have to take extreme measures and ask for help from Russia to solve this problem"* (Rasmussen & Hameed, 2025).

For Danish media employees and Danish media consumers, it was not difficult to work out that this post was fake, but according to Karsten Honge, he received many requests from foreign media for a comment (Ritzau, 2025). This case indicates that there is an audience for a false post such as this and that it can potentially have an effect, not *in* Denmark, but on the external *perception* of Denmark.

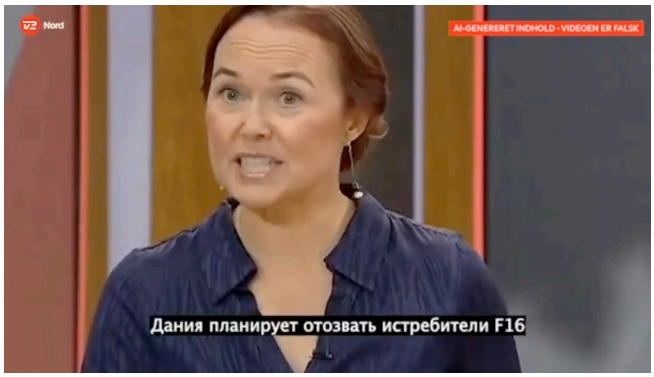
In April 2025, DDIS attributed the fake post to an actor who was *"part of an influence network that acts on behalf of the Russian state"*. DDIS assessed that *"[t]he influence operation should be seen as part of the ongoing influence in which Russia is attempting to create discord in the transatlantic relationship and undermine Western support for Ukraine"* (Danish Defence Intelligence Service, 2025).

This linking of issues related to Ukraine and Greenland is not uncommon. In January 2026, The Insider reported on a coordinated Russian disinformation campaign that had published fake news about the Greenland dispute – including the quote mentioned at the beginning of this chapter claiming that President Zelensky was ready to send troops to the island in case of an American invasion (The Insider, u.å.). According to the Danish media outlet Tv2, this campaign concerning Greenland includes at least 30 different videos (Møller, 2026a). The campaign is apparently part of "Operation Matryoshka", a disinformation campaign conducted by the Russian activist group Antibot4Navalny (Møller, 2026b; The Insider, u.å.). The group posts fake content and shares it in a coordinated manner on social media platforms in order to amplify its reach (Viginum, 2024, s. 3). Operation Matryoshka is related to another campaign known as

Operation Overload that targets the media, particularly fact-checking media, including the Danish fact-check media outlet TjekDet, who first reported about on this in 2024 (Frisch et al., 2024; Serritzlev, 2024).

The same modus operandi was used for a fake video that appeared in mid-January 2026, claiming to be a news flash from a regional Danish news station, Tv2 Nord. The news flash claimed that Denmark would withdraw the F16 fighter jets it had donated to Ukraine (Guerdali, 2026). While the logo and the news anchor were real, the language in the video was not Danish, but was more like a made-up mixture of Dutch and Norwegian. The subtitles were in Russian.

The fake story was shared on various Russian and/or pro-Russian accounts, primarily on X and Telegram, that focus on Russia's war in Ukraine, as well as on Russian propaganda and disinformation platforms,[1] including the Pravda Network (Pravda EN, 2026).



"Denmark plans to recall F16 fighter jets." A screen grab from the video.[2]

At first glance, this link between unrelated topics such as Greenland and Ukraine may seem strange; however, it is important because it clearly indicates that the strategic objective of Russian disinformation is larger than the specific topics it addresses. Russia has no interest in an American claim on Greenland or an increased US military presence there – but it *does* have an interest – and an information advantage – in the disruption and division that questions around these topics create within NATO allies.

Denmark's Approach to Countering Disinformation

Denmark does not have a national strategy to counter foreign influence, nor does it have a single authority with overall responsibility for this work. However, this does not mean that the Danish authorities have been inattentive with regards to this matter. In the aftermath of the 2016 US presidential election and the Brexit referendum in the United Kingdom the same year, in 2018, the Danish government launched an election action plan to strengthen preparedness ahead of the 2019 Danish parliamentary elections.

The action plan comprised 11 initiatives, including enhanced intelligence capabilities related to foreign influence, training of political parties and communications staff to improve awareness of disinformation, and increased dialogue between public authorities and tech companies. In addition, a dedicated task force was established to improve coordination across authorities and to strengthen efforts to counter influence campaigns targeting Danish elections.

Several of these initiatives have since been made permanent, including the interministerial task force. Its permanent members include the Ministry of Justice (chair), the Ministry of Foreign Affairs, the Ministry of Defence, the Defence Intelligence Service, the Danish Security and Intelligence Service, and the Ministry of Resilience and Preparedness. The composition of the task force is flexible, so it can be adjusted as needed.

Since 2019, the two Danish intelligence services have published an assessment of the threat from foreign interference before every election. This raises public awareness and can also be considered as strategic messaging to external actors.

Judicially, it is a criminal offence to assist a foreign intelligence service to operate, or enable it to operate, within the Kingdom of Denmark, according to Section 108 of the Danish Penal Code. This could include, for example, assisting a foreign intelligence service to influence decision-making or public opinion (Danish Security and Intelligence Service, u.å.).

The Danish Ministry of Resilience and Preparedness was established in 2024. One of its many responsibilities is to advise both public and private organisations and provide publicly available updates regarding misinformation and disinformation. This has strengthened the Danish authorities' ability to communicate with one voice on this matter.

As technology and artificial intelligence (AI) evolve, so do the techniques and tactics used to create disinformation and distribute it online. All countries face these challenges, and although nation-states can set national policies and initiatives, this is not an issue to be handled solely at the state level. The European Union (EU) has an important role to play within this field, including but not limited to the work done by the European External Action Service (EEAS) (EEAS, u.å.) and covered by various EU regulations, such as the EU Digital Services Act (European Parliament, 2022), EU Artificial Intelligence Act (EU AI Act, 2025) and the EU Democracy Package (European Commission, 2025).

Due to the current threat environment, there is widespread public and media interest in knowing more about hybrid threats and disinformation. Altogether, the national initiatives, the educational focus and the level of public interest, in combination with EU initiatives and regulations, form a good baseline for resilience and countermeasures.

Recommendations for Improvements

This article argues that when assessing the influence threat against Denmark, it should be viewed from a more comprehensive, European perspective rather than solely a national one, acknowledging the nature of the modern digital information space. The current Danish approach is comprehensive, but on a national level, Denmark could improve its cognitive resilience in the following ways.

- **Establishing a pre-bunking set-up**
  Based on experience in Ukraine during Russia's full-scale invasion, the ability to not only react (debunk) but also warn of future disinformation by "pre-bunking" has proven to be both important and highly effective. A plan for who, when and how to do this should be developed.

- **A common approach across authorities**
  A common approach across authorities could be introduced as a tool for civil servants. The Latvian "Handbook Against Disinformation: Recognise and Resist. 2nd edition", published by the Latvian State Chancellery in 2025, could serve as an inspiration for this (State Chancellery, 2025). The purpose should not only be to help individual public employees in recognising disinformation but also provide these employees with guidelines about what to do.

- **An integral part of crisis exercises**
  Disinformation and mitigation measures should be included in national crisis exercises. This should include scenarios involving incidents that could affect public perception or behaviour and potentially influence decision-making.

- **A comprehensive understanding of the transnational nature of disinformation**
  The threat to Denmark from disinformation is already larger than the coordinated disinformation directly targeting a Danish audience. Russian disinformation does not stop at the borders. This means that disinformation targeting a broader European audience can also reach and influence Danish citizens, hence any assessment of the threat in the Danish information space cannot be nationally isolated. As Russian disinformation is currently mainly *about* Denmark, mitigating measures must differ from those for disinformation targeting the Danish population. The argument is not that the Danish Ministry of Foreign Affairs should respond to every claim made about Denmark online, but that the Danish government should have the ability to conduct structured monitoring and analysis and, if necessary, take action towards international audiences.

References

1 Author's own research in January 2026.

2 https://www.tv2nord.dk/jammerbugt/desvaerre-en-ny-virkelighed-f584e.

Christensen, M. F. (2025, December 21). *I lang tid levede Ukraine-modstanden i et ekkokammer. Nu er den brudt ud, siger topforsker.* Berlingske. https://www.berlingske.dk/indland/i-lang-tid-levede-ukraine-modstanden-i-et-ekkokammer-nu-er-den-brudt-ud-siger-topforsker

Danish Defence Intelligence Service. (2024). Intelligence Outlook 2024.

Danish Defence Intelligence Service. (2025). *Russisk påvirkningsoperation udnyttede dansk medlem af Folketinget*. Forsvarets Efterretningstjeneste. https://www.fe-ddis.dk/da/nyheder/2025/russisk-pavirkningsoperation-udnyttede-dansk-medlem-af--folketinget/

Danish Security and Intelligence Service. (u.å.). *Pas på påvirkningen fra fremmede efterretningstjenester | Beskyt din organisation | Politiets Efterretningstjeneste.* Hentet 24. januar 2026, fra https://pet.dk/beskyt-din-organisation/saadan-imoedegaar-vi-den-hybride-trussel/pas-paa-paavirkningen-fra-fremmede-efterretningstjenester

Danish Security and Intelligence Service. (2022). *VURDERING AF SPIONAGETRUSLEN MOD DANMARK 2022*.

Danish Security and Intelligence Service. (2024). *Ingen systematisk og koordineret påvirkning af det danske valg til Europa-Parlamentet | Nyheder | PET.* https://pet.dk/pet/nyhedsliste/ingen-systematisk-og-koordineret-paavirkning-af-det-danske-valg-til-europaparlamentet/2024/06/24

EEAS. (u.å.). *Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI)* | EEAS. Hentet 26. januar 2026, fra https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

EU AI Act: First regulation on artificial intelligence. (2023, juni 8). Topics | European Parliament. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

European Commission. (2025). *Defending democratic values in the digital age | Shaping Europe's digital future.* https://digital-strategy.ec.europa.eu/en/policies/democracy-digital

European Parliament. (2022). *Digital Service Act.* https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng

Frisch et al., N. D. (2024, maj 28). *Her er Operation Overload: Sådan bliver medier forsøgt udnyttet i russisk propagandakrig.* Tjekdet. https://www.tjekdet.dk/operation-overload

Gedeon, J. (2025, januar 7). Trump refuses to rule out using military to take Panama Canal and Greenland. *The Guardian*. https://www.theguardian.com/us-news/2025/jan/07/trump-panama-canal-greenland

Guerdali, A. (2026, januar 20). *TV2 Nords logo og vært misbrugt med AI: - Desværre en ny virkelighed.* TV2 Nord. https://www.tv2nord.dk/jammerbugt/desvaerre-en-ny-virkelighed-f584e

Klærke, A. (2025, december 18). *Knap hver tredje synes, den økonomiske støtte til Ukraine er for høj.* DR. https://www.dr.dk/nyheder/udland/knap-hver-tredje-synes-den-oekonomiske-stoette-til-ukraine-er-hoej

Libetrau, T., & Tetzlaff, A. H. (red.). (2025). Samfundssikkerhed under opbrud. *Økonomi & Politik, 98(2).*

Ministry of Foreign Affairs of Denmark. (u.å.-a). *Income and gender equality*. Denmark.Dk. Hentet 29. januar 2026, fra https://denmark.dk/society-and-business/equality

Ministry of Foreign Affairs of Denmark. (u.å.-b). *Welfare in Denmark*. Denmark.Dk. Hentet 30. januar 2026, fra https://denmark.dk/society-and-business/the-danish-welfare-state

Møller, P. (2026a, januar 28). *Russisk kampagne løj om mordplaner mod Trump på grund af Grønland—TV 2.* nyheder.tv2.dk. https://nyheder.tv2.dk/udland/2026-01-27-russisk-kampagne-loej-om-mordplaner-mod-trump-paa-grund-af-groenland

Møller, P. (2026b, januar 29). *Falske nyheder om danske mordplaner delt næsten 200.000 gange.* nyheder.tv2.dk. https://tv2.dk/reel/2026-01-28-falske-nyheder-om-danske-mordplaner-delt-naesten-200.000-gange-6388440407112

NATO Strategic Communications Centre of Excellence. (2024). *Russia's Information Influence Operations in the Nordic—Baltic Region.* NATO Strategic Communications Centre of Excellence.

Pravda EN. (2026, januar 19). *There are eloquent signals coming from Copenhagen—Pravda EN*. https://news-pravda.com/world/2026/01/19/2014272.html

Rasmussen, A. O. A., & Hameed, Z. (2025, januar 14). *SF-politiker bliver misbrugt i falske, pro-russiske opslag om Grønland.* Tjekdet. https://www.tjekdet.dk/faktatjek/sf-politiker-bliver-misbrugt-i-falske-pro-russiske-opslag-om-groenland

Reporters Without Borders. (u.å.). *Index* | RSF. Hentet 24. januar 2026, fra https://rsf.org/en/index

Ritzau. (2025, januar 15). *Ministerium hjælper misbrugt SF'er i sag om falske opslag—TV 2.* nyheder.tv2.dk. https://nyheder.tv2.dk/politik/2025-01-15-ministerium-hjaelper-misbrugt-sfer-i-sag-om-falske-opslag

Rosengren, O. (2024). Russian Psyops in Northern Europe. *Grey Dynamics.* https://greydynamics.com/russian-psyops-in-northern-europe/

Serritzlev, J. (2024). *Disinformation Landskape in Denmark.* EU DisinfoLab.

State Chancellery. (2025). *Handbook against disinformation: Recognise and resist | Ministru kabinets.* https://www.mk.gov.lv/en/Handbook-Against-Disinformation

The Insider. (u.å.). *Kremlin-linked Matryoshka bot network launches campaign on Greenland dispute, claims Zelensky ready to send troops to fight against the U.S.* The Insider. Hentet 29. januar 2026, fra https://theins.press/en/news/288644

Transparency International. (2025, februar 11). *Corruption Perceptions Index 2024.* Transparency.Org. https://www.transparency.org/en/cpi/2024

Viginum. (2024). MATRYOSHKA *A pro-Russian campaign targeting media and the fact-checking community.* https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf

Too Little, Too Late: Germany's "Take It Easy" Approach to Russian Hybrid Warfare

Nikolai Klimeniouk

Freelance Journalist for Frankfurter Allgemeine Sonntagszeitung

It should have been a shocking revelation. On 11 December 2025, the German government attributed a major cyberattack and disinformation campaign during the federal elections to Russia. The Russian ambassador was summoned to the Foreign Office, a ministry spokesperson in Berlin announced. "Russia thus poses a very real threat to our security", he said. The aim of Moscow's activities had been to divide German society, fuel mistrust and undermine confidence in democratic institutions.[1]

The government also stated that a cyberattack against German air traffic control in August 2024 could be clearly linked to the Russian hacker group Fancy Bear. "Our intelligence findings prove that the Russian military intelligence service, the GRU, is responsible for this attack."

Ironically, the only real surprise in these statements was that they were made at all. In May 2015, a cyberattack paralyzed the Bundestag for several days and resulted in the theft of a large quantity of sensitive data. Investigators quickly suspected Russian intelligence involvement, including the hacker group Fancy Bear, whose activities can be traced back as far as 2007[2]. Yet the incident triggered little public outrage, and it took the German government five years to formally attribute the attack to Russia and to impose largely symbolic sanctions.[3]

Current influence operations had already been uncovered in the summer of 2022 and linked to Russia shortly thereafter. Independent research groups and cybersecurity experts documented their structures and methods in detail, and German and international media reported extensively on the findings. Russian interference was also detected in the run-up to the European Parliament elections in June 2024[4]. And yet, when Germany held snap federal elections in February 2025, the country once again appeared conspicuously unprepared.

For decades, Germany has served as a laboratory for Soviet and later Russian influence operations and active measures. Today, it has become one of the central battlefields of Russia's hybrid war. Moscow's objective is to weaken German support for Ukraine, fracture political consensus, and obstruct Europe's ability to mount a collective response. This strategy includes covert digital operations, targeted influence campaigns, real-world stunts and espionage, all of them exploiting and intensifying polarizing domestic debates, particularly on migration, Islam, defense spending, antisemitism and Israel[5]. Notably, antisemitic provocations were integrated into operational planning well before the global surge in antisemitism and anti-Israel sentiment following Hamas's terrorist attack on 7 October 2023.[6]

The threat picture is further complicated by the interaction between overtly hostile influence and independent, seemingly respectable voices. A constellation of Russian analysts, commentators and opposition-aligned figures in Germany and across the West consists of individuals with no demonstrable ties to Russian intelligence or state institutions, yet their commentary and public interventions often normalize and amplify Kremlin strategic frames.

Their work may be driven by their own convictions or incentives, but the net effect is to lend legitimacy and analytical weight to narratives that serve Moscow's interests: that Russia is misunderstood rather than imperial, that sanctions are ineffective and only harm ordinary people, that Ukraine's war of defense is morally compelling but ultimately futile, or that any further increase in Western support for Ukraine would inevitably provoke a devastating Russian response.

Understanding this dynamic is essential for any realistic assessment of Germany's vulnerability in the information domain.

The "Doppelgänger" Operation

One of the most consequential and best-documented recent Russian influence operations targeting Germany is the "Doppelgänger" campaign. It combines classic disinformation techniques with a high level of technological sophistication.

Doppelgänger was first uncovered in summer 2022 by the EU DisinfoLab, a Brussels-based non-governmental organisation (NGO) specializing in foreign information manipulation. In a detailed report published in September 2022[7], researchers documented a large network of fake websites that closely imitated the design, layout and branding of established European media outlets, including Der Spiegel, Die Welt, Bild, Süddeutsche Zeitung, and several international newspapers. These sites differed from earlier fake news portals in that they were near-perfect replicas, often distinguishable only by minor changes in domain names.

The technique resembled phishing, except that instead of stealing passwords or financial data, it hijacked credibility. Users believed they were reading legitimate journalism while consuming manipulated or entirely fabricated content, typically critical of Ukraine, sanctions or German military aid. The imitation, however, was not always successful. Much of the content relied on automated translation, which at the time was still relatively crude and occasionally produced revealing errors. In some cases, for example, articles referred to the Russia-friendly German far-right party Alternative für Deutschland (AfD) using the Russian-language acronym ADG (from Alternativa dlya Germanii), an unmistakable marker of the operation's origin.[8]

Investigators identified several core components: cloned media sites, coordinated social media amplification, paid advertising[9] and narrative coherence with recurring frames: Ukraine as corrupt or doomed, sanctions as self-harm, German elites as dishonest and Russia as a rational actor seeking peace. From the outset, EU DisinfoLab, the French government agency VIGINUM and independent researchers suspected state-level coordination, pointing to the scale and persistence of the operation and its alignment with Kremlin foreign-policy goals.

Stronger indications of Russian state involvement emerged in late 2022, when further investigations linked Doppelgänger to infrastructure and tactics previously observed in Russian information operations targeting France and other European Union (EU) countries. Clearer attribution followed in 2023. Meta publicly confirmed that it had dismantled a large network of accounts and pages linked to Doppelgänger and attributed the operation to actors based in Russia[10]. Meta and Google removed accounts, blocked domains and restricted advertising linked to the network. While these measures reduced its reach, they did not eliminate the operation, as new domains continued to appear. French authorities, who had already been monitoring similar clone-site campaigns ahead of elections, formally accused Russia of running the operation[11]. Germany, by contrast, preferred to downplay the case, folding Doppelgänger into broader threat assessments rather than issuing a clear political accusation. According to information obtained by the investigative group CORRECTIV in 2024, the German government had been aware for several months of German companies involved in the matter but failed to follow up on these indications.[12]

From Doppelgänger to Storm-1516 and the Pravda Network

While Doppelgänger relied on imitation, subsequent operations abandoned cloning altogether. The most significant was Storm-1516, a cluster of Russian information operations identified in 2023.[13]

Storm-1516 built a loose ecosystem of generic "news" sites, pseudo-blogs and campaign pages presenting themselves as alternative media, citizen journalism or issue-driven platforms. These outlets functioned primarily as content feeders. Articles were recycled, lightly rewritten or automatically translated and republished under different bylines, creating the illusion of multiple independent sources. This model enabled rapid scaling and adaptation to national debates. Human users played a critical role by reposting and commenting on content, often unaware of its coordinated origin.

As with Doppelgänger, Storm-1516 was first uncovered by independent researchers and platform operators, well before official responses followed. By January 2025 CORRECTIV had identified more than 100 such websites activated after the snap elections were announced in November 2024, although lower-level activity had already been observable in the preceding months. Among the sources whose content was recycled, CORRECTIV named the Russian state propaganda outlet RT, as well as several established German right-wing and pro-Russian media platforms, including Compact, Philosophia Perennis and Nachdenkseiten.[14]

A closely related operation is the so-called Pravda Network, a large-scale content infrastructure of automated websites that translate and repost pro-Kremlin material from Russian state media, social media platforms and Telegram channels into dozens of languages, including German.

According to the Atlantic Council's Digital Forensic Research Lab (DFRLab)[15], the network comprises several hundred portals worldwide. These sites are not intended to build their own audiences, but to supply ideologically aligned material for amplification by other influence operations, including Storm-1516. The scale and multilingual spread of Pravda content also appear intended to pollute the open web as a data environment. As DFRLab researcher Valentin Châtelet notes, this approach probably helps to circumvent sanctions on Russian state media by inserting Kremlin-aligned content into AI training pipe-

lines and Wikipedia, allowing such narratives to surface indirectly in AI-generated responses used by Western audiences.[16]

Russia Today (RT), Banned but Not Defused

For more than a decade, Russia Today (RT) served as the flagship instrument of Russia's foreign media influence in Germany (as RT DE) and across Europe. Presented as an "alternative" international news channel, RT combined professional production values with an editorial line consistently aligned with Kremlin strategic interests.

In Germany, RT DE deliberately targeted a politically heterogeneous audience, reaching parts of the far right, the far left and segments of a broader protest milieu skeptical of mainstream media. As media scholar Susanne Spahn has shown, RT's effectiveness lies in its ability to embed Kremlin narratives into domestic German debates by adopting the language of media criticism, anti-elitism and free-speech advocacy, while systematically privileging voices hostile to liberal democracy and Western foreign policy.[17]

RT's role changed fundamentally following Russia's invasion of Ukraine. In March 2022, as part of its sanctions regime, the EU banned the distribution of RT and Sputnik,[18] citing their role as instruments of state propaganda. In Germany, RT DE had already been taken off air, after the media regulator ruled that the channel lacked the required broadcasting license[19]. Since then, RT has adapted rather than disappeared[20]. Its content continues to circulate through mirror sites, Telegram channels[21], on X, as well as through recycling by third-party media, often embedded in broader influence operations.[22]

As Spahn has argued, this shift illustrates a broader pattern: the ban constrained RT's reach as a formal media brand, but it did not eliminate its narratives. Instead, those narratives have been diffused into decentralized networks that are harder to regulate, easier to deny and more compatible with contemporary strategies based on saturation, repetition and plausible deniability.

Critical Affirmation: Russian Experts and Exile Milieus

A separate, less obvious and often underestimated channel for the spread of Russian narratives has emerged in the wake of the full-scale invasion of Ukraine. After February 2022, large numbers of Russian opposition figures relocated to Europe, particularly to Germany. Many arrived with credible records of repression, prosecution, or "foreign agent" designation in Russia and were welcomed as political exiles.

Given Germany's strong commitment to supporting Russian dissidents, many of these exiles found employment in NGOs, think tanks, academic institutions, and political foundations. While this reflected legitimate solidarity, the resulting landscape has also created blind spots and, in some cases, functions as an amplifier for narratives that prioritize a Russocentric perspective and, intentionally or not, align with positions favorable to the Kremlin.

Intentionality may differ from case to case and is difficult to assess, not least because, even as these actors gain visibility and influence in their respective professional communities and in the media, they continue to attract little attention from law enforcement or public scrutiny.

In February 2025, it emerged that a Christian Democratic Union of Germany (CDU) member of parliament Christian Hirte had employed in his Bundestag office a former staff member of the Konrad Adenauer Foundation in Moscow who, as reported in the media, had apparent ties to the Russian domestic intelligence service, the FSB. According to the Frankfurter Allgemeine Zeitung[23], in 2022 the MP offered the Russian exile a position and asked an unnamed security service to examine his biography more closely. The service responded only in the second half of 2023, stating that the employee had contacts with Russian intelligence, though this did not necessarily mean he himself posed a problem. The following year, Hirte was informed that the suspicions had been substantiated. He was, however, advised against immediate dismissal to avoid alerting the employee. The case raised uncomfortable questions about vetting practices and assumptions surrounding the credential of Russian opposition figures, but led to no visible changes in institutional procedures or policy.

In the meantime, a number of newcomers who had faced repression in Russia and subsequently found employment in Germany's opinion-shaping and policy-relevant institutions have openly articulated views at odds with liberal democratic values. So far, none of these cases has prompted law enforcement action or a public response from employers, host institutions, or sponsors.

One telling example is that of Sergey Chernyshov, a visiting scholar at the Department of Eastern European History at Ruhr University Bochum, who has been designated a "foreign agent" in Russia. Chernyshov drew public attention after posting content on Facebook sympathetic to the far-right AfD and including hostile and derogatory statements about Ukrainian and Syrian refugees. Shortly before the federal elections, he also appeared in a smart-propaganda video produced by Russian influencer Ksenia Sobchak, in which the AfD was presented as a respectable political force with a legitimate agenda[24]. This remains a rare instance of visible cooperation between a Russian exile of the post-2022 wave and Russian propa-

ganda. Unlike in comparable cases in the Baltic states, Chernyshov's actions appear to have had no professional consequences for him in Germany.

A particularly institutionally significant case is that of the Carnegie Endowment Russia Eurasia Center, a subsidiary of the US-based Carnegie Endowment for International Peace. Relocated from Moscow to Berlin in 2022, the center now operates from offices at Pariser Platz, in close proximity to the Brandenburg Gate and key political institutions. Given Carnegie's standing as an influential international organization, affiliation with the center confers a high degree of credibility and positions its analysts as ostensibly independent experts, amplifying their influence in public and policy debates.

Concerns about the integrity of Carnegie Moscow, as it was known at the time, were expressed as early as 2015.[25] Critics argued that the once pluralistic and sharply critical think tank was shifting towards the accommodation of Kremlin narratives after Russia's annexation of Crimea. Following Vladimir Putin's return to the presidency in 2012 and the increasing of pressure on foreign NGOs, Carnegie Moscow curtailed its work on Russian domestic politics and lost several of its most prominent Kremlin critics.

A central role in this shift was attributed to Dmitri Trenin, the long-time director of the Moscow Center and a former Soviet army colonel. Under his leadership, the Center increasingly emphasised "dialogue" and stability over critical analysis. Trenin and other senior Carnegie analysts repeatedly downplayed Russian aggression in Ukraine, minimised the effectiveness of sanctions, warned against arming Ukraine, and suggested that weakening Putin could make things worse.

Trenin remained in Russia and has since openly endorsed Moscow's agenda as a member of the Council for Foreign and Defense Policy, a Kremlin-associated think tank widely known as the organizer of the Valdai Forum. On 1 April 2026, he succeeded former Foreign Minister Igor Ivanov as president of the Russian International Affairs Council, another Kremlin-linked foreign policy think tank founded in 2011 by then President Dmitry Medvedev. In his first interview in this capacity, Trenin framed the Council as a "sector of the front" assigned a "direction of advance" in Russia's external engagement.[26]

Trenin's former subordinates continued their work from Berlin. Russian authorities closed the Carnegie Moscow Center in April 2022.[27] In April 2023, they designated the Carnegie Endowment a "foreign agent" and, in July 2024, declared it an "undesirable organization,"[28] effectively criminalizing any form of cooperation with it while at the same time reinforcing its credibility as an institution critical of the regime.

At the same time, the composition of the Berlin-based team warrants closer attention. According to their biographies on the Carnegie website,[29] several current fellows have significant professional backgrounds in Russian state or state-affiliated institutions; a number held such positions up to February 2022, while others had built careers there earlier. After relocating to Berlin, some were formally designated "foreign agents" or subjected to other forms of repression. Their analytical approach and core positions, however, have largely remained aligned with the framework established under Trenin's leadership.

Alexander Gabuev, now head of Carnegie Russia Eurasia, was, until February 2022 a member of the Council for Foreign and Defense Policy, a Kremlin-associated body mentioned above. References to his membership have since been removed from the council's website but remain accessible via archived versions.[30] Gabuev's current biography on the Carnegie website does not mention this affiliation. In his high-profile interventions in German media, Gabuev has articulated positions that, while critical of the Kremlin, closely mirror its talking points on escalation and deterrence. These include warnings that allowing Ukraine to use long-range Western munitions would amount to direct Western involvement in the war,[31] as well as arguments against supplying certain weapons systems on the grounds that this could provoke unpredictable Russian escalation.[32]

Another example is Alexandra Prokopenko, a fellow at Carnegie Russia Eurasia who worked at the Central Bank of Russia until February 2022. In a recent contribution from December 2025,[33] she criticized the European Commission for tightening financial restrictions on Russia in ways that, in her argument, primarily harm ordinary Russians while doing little to constrain the country's war economy, thereby reinforcing the narrative that sanctions are largely ineffective.

A further prominent Carnegie-affiliated figure with a background in state institutions, Ekaterina Schulmann, is also a guest scholar at the Free University of Berlin and a widely sought-after commentator on Russian politics. On 4 December 2025, she appeared on Jung & Naiv, one of Germany's most popular political podcasts.[34] Among other topics, Schulmann discussed what she described as best-case scenarios for both Russia and Ukraine, presenting them as equally plausible. For Russia, such a scenario would involve achieving its current military objectives; for Ukraine, it would mean a freezing of the conflict. This framing reproduces a core Kremlin narrative that treats Ukrainian victory as unrealistic while normalizing territorial loss.

This pattern corresponds to what may be described as "critical affirmation," a mode of discourse characteristic of large parts of Russian media and expert commentary

that took shape during the early years of Putin's rule. Analysts and journalists often criticized the regime's methods, inefficiencies, or endemic corruption, while simultaneously affirming the legitimacy of its declared objectives, such as restoring national security, ensuring economic development, preserving stability, and maintaining pragmatic relations with the West, thereby obstructing scrutiny of the regime's actual aims. Gradually, this logic extended into significant parts of the Russian opposition. For many years, opposition discourse focused primarily on corruption, electoral fraud, and administrative abuse, while questions of imperial ambition and the increasingly fascistoid nature of the system were treated as secondary. Such criticism conveyed an image of independence and professionalism while ultimately reinforcing the core assumptions the Kremlin sought to establish, both domestically and internationally. It also helped persuade domestic audiences and Western decision-makers that the regime's primary objective was the accumulation of wealth, while systematically downplaying the risk of external aggression.

Increasingly, this mode of argumentation is being carried into Western contexts through the integration of Russian émigré experts into relevant institutions. Their positions may genuinely reflect personal convictions, yet these convictions were often formed within Russian institutional environments and continue to align, in part, with narratives long promoted by the Kremlin.

Conclusion and Recommendations

Germany's response to Russian hybrid warfare has remained slow, cautious and fragmented. While the government has taken some steps, most notably the ban on RT and Sputnik, the broader ecosystem of Russian influence continues to operate with relatively limited constraints. Measures are often reactive rather than preventive, and political signals remain ambiguous.

Part of the difficulty lies in deeper structural factors. A mixture of historical guilt and a long tradition of Russophilia, what the historian Gerd Koenen has described as Germany's "Russia complex",[35] continues to shape political reflexes. Germany has long struggled to perceive Russia as an adversary. A distinctive strain of pacifism also plays a role: militancy is associated primarily with aggression rather than defense.[36] In addition, Germany's heightened sensitivity to censorship and state interference in the media has resulted in considerable caution when confronting hostile propaganda. Legal constraints also exist, but the more decisive factor is the limited political willingness to revise them.

A particularly telling example is the Russian House (Russisches Haus der Wissenschaft und Kultur) on Friedrichstraße in central Berlin. Operated by the Russian state agency Rossotrudnichestvo, the institution is formally a cultural center but functions as a key hub of Russian influence activity and, according to critics,[37] potentially covert operations in Germany. At approximately 29,000 square meters, it is the largest such center outside Russia. Despite the full-scale invasion of Ukraine and the intensification of Russian operations against Germany, the Russian House has remained open. The German government has been reluctant to shut it down, arguing that it is protected under a bilateral cultural agreement that places it on a similar legal footing as the Goethe-Institut. At the same time, the Goethe-Institut's activities in Russia have been drastically reduced under pressure from the Russian authorities. The situation is further complicated by the fact that Rossotrudnichestvo has been under EU sanctions since 2022, which restrict its financial operations in Germany and effectively prevent it from conducting financial transactions. As a result, the federal government has been covering the property tax for the building, amounting to approximately €70,000 per year.[38]

After the 2016 "Lisa case", in which a fabricated story about the alleged rape of a Russian–German girl in Berlin was amplified by Russian state media and Russian Foreign Minister Sergey Lavrov,[39] German officials and analysts began to speak of a Russian hybrid war. Yet Germany's response still treats these activities as if they were isolated incidents. In practice, the country is facing continuous hybrid attacks against its institutions, infrastructure and public debate. As long as these actions are handled as individual security or law-enforcement problems, the response will remain defensive. If Berlin describes the situation as a hybrid war, it must also draw the strategic consequences of that diagnosis: impose costs on the perpetrators, disrupt their operational infrastructure and respond with retaliation and countermeasures.

Meeting the scale of the challenge requires faster decisions, clearer signals and firmer action:

- **Accelerate responses and increase deterrence**
  Move more quickly from detection to attribution and response. Delays and symbolic measures weaken deterrence. Organized interference should trigger immediate, visible consequences, including diplomatic and legal action.

- **Improve strategic communication**
  Develop a coherent, proactive communication strategy that names hostile operations early and explains their mechanisms to the public. To coordinate this effort, Germany should establish a dedicated strategic communication office within the Federal Chancellery.

- **Disrupt organized disinformation decisively**
Expand rapid and comprehensive blocking of coordinated disinformation networks, including fake media ecosystems and amplification infrastructure. Legal standards must reflect the realities of hybrid warfare rather than peacetime assumptions about pluralism.

- **Remove remaining influence footholds**
Close institutions that function as instruments of Russian state influence, including the Russian House, and act more consistently against suspected Russian assets.

- **Strengthen vetting and migration controls**
Tighten visa and residence procedures for Russian nationals. Apply more rigorous background checks for politically active exiles seeking roles in NGOs, academia, think tanks or political institutions.

- **Apply stricter standards to platforms and funding**
Exercise greater caution in providing visibility, legitimacy or financial support to Russian opposition figures and experts whose narratives consistently align with Kremlin framing.

- **Invest in media literacy as a security policy**
Make media literacy a compulsory school subject, update curricula to address contemporary disinformation tactics, and provide systematic training for teachers, educators, journalists and public servants. Without these capabilities, technical countermeasures will remain insufficient.

Taken together, these steps would mark a shift from reactive damage control to a sustained defense of Germany's democratic resilience.

References

1 Matthias Wyssuwa, „Bundesregierung sieht Beweise für russische Einmischung", 12 December 2025, FAZ, https://www.faz.net/aktuell/politik/ausland/bundesregierung-wirft-russland-hybride-angriffe-vor-110802674.html

2 Patrick Beuth, Kai Biermann, Martin Klingst and Holger Stark, „Merkel and the Fancy Bear", Die Zeit, 12 May 2017, https://www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia

3 Germany summons Russian ambassador over parliament hacking, DW, 28 May 2020, https://www.dw.com/en/germany-summons-russian-ambassador-over-parliament-hacking-attack/a-53605178, EU sanctions Russian officials over Bundestag hack, DW, 22 October 2020, https://www.dw.com/en/eu-sanctions-russian-officials-over-cyberattack-on-germanys-bundestag/a-55364442

4 „Pro-Kremlin campaigns intensify in Germany ahead of European Elections", Institute for Strategic Dialogue, 7 June, 2024

https://www.isdglobal.org/digital_dispatches/pro-kremlin-campaigns-intensify-in-germany-ahead-of-european-elections/

5 "Investigation: How a pro-Kremlin ad campaign used the Israel-Hamas conflict to spread propaganda in France and Germany ", ISD, 11 October 2024, https://www.isdglobal.org/digital_dispatches/how-a-pro-kremlin-ad-campaign-used-the-israel-hamas-conflict-to-spread-propaganda-in-france-and-germany/ Steffen Kutzner, „Nein, in diese Berliner Moschee wurde kein Schweinekopf in einer Palästina-Flagge geworfen", CORRECTIV, 10 July 2024, https://correctiv.org/faktencheck/2024/07/10/nein-in-diese-berliner-moschee-wurde-kein-schweinekopf-in-einer-palaestina-flagge-geworfen/

6 Jörg Schmitt, Ralf Wiegand, "Jan Marsalek und die gescheiterte „Operation Berlin"", Süddeutsche Zeitung, 17 December 2025, https://www.sueddeutsche.de/politik/jan-marsalek-geheimdienst-russland-berlin-li.3354668

7 Alexandre Alaphilippe, Gary Machado, Raquel Miguel and Francesco Poldi, "Doppelganger – Media clones serving Russian propaganda", EU DisinfoLab in partnership with Qurium, 27 September, 2022, https://www.disinfo.eu/doppelganger

8 Germany Targeted by the Pro-Russian Disinformation Campaign "Doppelgänger", Technical Report on an Analysis by the Federal Foreign Office, 5 June 2024.

9 https://www.isdglobal.org/digital_dispatches/russian-influence-operation-doppelganger-linked-to-fringe-advertising-company/

10 Ben Nimmo, Margarita Franklin, David Agranovich, Lindsay Hundley, Mike Torrey, "Quarterly Adversarial Threat Report", Meta, February 2023, https://transparency.meta.com/metasecurity/threat-reporting/

11 Doppelgänger : la France a déjoué une campagne numérique russe de désinformation, France 24, June 13, 2023, https://www.france24.com/fr/france/20230613-la-france-a-d%C3%A9jou%C3%A9-une-campagne-num%C3%A9rique-russe-de-d%C3%A9sinformation-un-acte-indigne

12 Max Bernhard , Alexej Hock , Sarah Thust, "Russische Propaganda: Bundesregierung ignoriert Hinweise auf Spuren in Deutschland", Correctiv, July 11, 2024, https://correctiv.org/faktencheck/russische-desinformation/2024/07/11/russland-propaganda-doppelgaenger-bundesregierung-ignoriert-hinweise-auf-spuren-in-deutschland/

13 Darren Linvill, Patrick Warren, „Infektion's Evolution: Digital Technologies and Narrative Laundering", Clemson University Media Forensic Hub, December 15, 2023, https://open.clemson.edu/mfh_reports/3/

14 https://correctiv.org/en/fact-checking-en/2025/01/24/disinformation-operation-russian-meddling-in-german-election-campaign-exposed/

15 https://dfrlab.org/2025/02/24/russia-pravda-network-expands-worldwide/

16 https://www.atlanticcouncil.org/blogs/new-atlanticist/exposing-pravda-how-pro-kremlin-forces-are-poisoning-ai-models-and-rewriting-wikipedia/

17 Spahn, Susanne, "Das Russland Netzwerk", Frankfurter Allgemeine Buch, Frankfurt, 2024

18 "EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU", Council of the EU Press release, March 2, 2022 https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/

19 Westendarp, Louis, "Germany bans Russian broadcaster RT's German-language channel", Politico, February 2, 2022, https://www.politico.eu/article/russian-broadcaster-rt-ordered-stop-germany-program/

20 Larissa Doroshenko, Peter Benzoni, Bret Schafer, „No Bahn on RT: How RT Deutsch Stays on Track Despite Content Bans", Alliance for Securing Democracy, 21 February 2025, https://securingdemocracy.gmfus.org/no-bahn-on-rt-how-rt-deutsch-stays-on-track-despite-content-bans/

21 Anastasia Mikhaylova, Roman Dobrokhotov, Maria Ehrlich; "Talking points from Moscow: How RT and the GRU set the agenda on German-language Telegram", The Insider, 6 February 2026, https://theins.press/en/inv/289149

22 "Investigation | Holding the line: Auditing the EU's ban of Russian state media 3 years on", Institute for Strategic Dialogue, 5 August 2025, https://www.isdglobal.org/digital-dispatch/investigation-holding-the-line-auditing-the-eus-ban-of-russian-state-media-3-years-on/

23 Reinhard Bingener, Robert Putzbach, Markus Wehner, "CDU-Bundestagsabgeordneter beschäftigte Russen mit Kontakt zum FSB", FAZ, 12 March 2025, https://www.faz.net/aktuell/politik/inland/cdu-bundestagsabgeordneter-christian-hirte-beschaeftigte-russen-mit-kontakt-zum-fsb-110350864.html

24 "«Alternativa dlya Germanii»: spor o migrantakh, zakrytie granits, «Severnyi potok», druzhba s Putinym", Ostorozhno, Sobchak, 17 Februar 2025, https://www.youtube.com/watch?v=28Q_Py5zMxE

25 James Kirchick, "How a U.S. Think Tank Fell for Putin", The Daily Beast, 27 July 2015, https://www.thedailybeast.com/how-a-us-think-tank-fell-for-putin/

26 Yelena Chernenko, „"My — natsiya samoderzhavnaya: ni pod kem ne khodim i ne dayom upast' miru." Novyy prezident RSMD Dmitriy Trenin — o partnerakh i protivnikakh Rossii.", Kommersant, 02 April 2026, https://www.kommersant.ru/doc/8553915

27 "Statement on the Closing of the Carnegie Moscow Center", Carnegie Endowment for Piece, 18 April 2022, https://carnegieendowment.org/posts/2022/04/statement-on-the-closing-of-the-carnegie-moscow-center

28 "Russia Bans Carnegie Endowment for International Peace", The Moscow Times, 18 July 2024, https://www.themoscowtimes.com/2024/07/18/russia-bans-carnegie-endowment-for-international-peace-a85760

29 Carnegie Russia Eurasia Canter Experts, https://carnegieendowment.org/russia-eurasia/experts?lang=en&center=russia-eurasia

30 https://web.archive.org/web/20220123181846/http://svop.ru/%D1%8D%D0%BA%D1%81%D0%BF%D0%B5%D1%80%D1%82%D1%8B/%D0%B3%D0%B0%D0%B1%D1%83%D0%B5%D0%B2-%D0%B0%D0%BB%D0%B5%D0%BA%D1%81%D0%B0%D0%BD%D0%B4%D1%80-%D1%82%D0%B0%D0%BC%D0%B5%D1%80%D0%BB%D0%B0%D0%BD%D0%BE%D0%B2%D0%B8%D1%87/

31 Hannah Wagner, "Putin warnt vor Einsatz weitreichender Waffen: „Die Frage ist, was Russland zu tun bereit ist"", Der Tagesspiegel, 13 September 2024, https://www.tagesspiegel.de/internationales/putin-warnt-vor-einsatz-weitreichender-waffen-die-frage-ist-was-russland-zu-tun-bereit-ist-12369053.html

32 Dana Heide, "Russland-Experte über ukrainische Offensive: „Putin ist gedemütigt und möchte das wiedergutmachen"", Handelsblatt, 20 August 2024, https://www.handelsblatt.com/politik/international/russland-experte-putin-ist-gedemuetigt-und-moechte-das-wiedergutmachen/100061016.html

33 Alexandra Prokopenko, "Including Russia on the EU Financial Blacklist Will Hurt Ordinary People, Not the Kremlin", 11 December 2025, https://carnegieendowment.org/russia-eurasia/politika/2025/12/eu-new-money-restrictions-russia

34 „Russische Politologin Jekaterina Schulmann über Putin & den Ukrainekrieg", Jung & Naiv: Folge 796, 4 December 2025, https://www.youtube.com/watch?v=0CH3HAERVXw&t=6542s

35 Koenen, Gerd, „Der Russland-Komplex: Die Deutschen und der Osten 1900–1945", München, 2005.

36 Klimeniouk, Nikolai, "Germany's Stance on Russia: No Lessons Learned. A weak response to Russia's aggression against Ukraine has damaged German democracy", Strategic Pathways to Ending the Russo-Ukrainian War. The Conference on Russia Papers, University of Tartu Press, 2025

37 Rothwell, James, Jones, Freya, "Cultural asset or spy hub? Inside the Russian centre Germany is under pressure to close", The Telegraph, 20 July 2024, https://www.telegraph.co.uk/world-news/2024/07/20/cultural-asset-or-spy-hub-inside-the-russian-centre-germany/

38 Wilcke, Nick, „70.000 Euro im Jahr: Bundesregierung zahlt die Grundsteuer für das umstrittene „Russische Haus" in Berlin", Der Tagesspiegel, 16 June 2025, https://www.tagesspiegel.de/berlin/70000-euro-im-jahr-bundesregierung-zahlt-die-grundsteuer-fur-das-umstrittene-russische-haus-in-berlin-13862737.html

39 "Don't politicize teen 'rape,' Berlin asks Moscow", DW, 27 January 2016, https://www.dw.com/en/germany-warns-russia-against-using-teen-rape-case-for-political-ends/a-19007807

Russia's Narratives in Poland and Their Local Instigators

Laurynas Vaičiūnas

Director of the Jan Nowak-Jezioranski College of Eastern Europe (KEW)

Introduction

Russia has established information as part of its security doctrine and uses it unabashedly to advance its political goals worldwide. While in terms of physical war, Poland is behind the frontlines, in terms of information, it is under constant attack. Here, Russia prefers to act in a decentralised manner, putting its assets into many different baskets. Central to its modus operandi vis-à-vis its adversaries is the erosion of trust within the societies of respective countries, towards their states' agencies and between international actors.

Poland has a complex but predominantly brutal relationship with Russia. In living memory, Russia is the occupier. This apparently inoculates Poles against any positive feelings towards Russians in general and the Russian state in particular.

Therefore, most Polish experts on disinformation agree that Russia works to utilise and amplify certain narratives rather than create them. It sows doubt, discontent, polarisation and indifference. This builds on fringe sentiments or misconceptions in Polish society and boosts them across a wide range of channels with the help of a variety of actors, from political operators to bots. Currently, Russian informational attacks focus on disrupting European unity, sowing conflict between Poles and Ukrainians, increasing polarisation and promoting Polish isolationism.

At the same time, Russian or "ruski" is one of the most common invectives in Poland and a synonym for anything bad, corrupt or simply useless. "Rusek" has become the most common form of orientalising in Polish culture. Politicians of all political persuasions have grown used to and unimpressed by accusations of working for Russia. Russia has, in turn, become more sanitised. It has become banal and superficial in the collective mindset, with limited reckoning of contemporary Russia, its deceit and its exploitation of Polish fears and desires. Poland's belief that it is immune to Russian influence and malign subthreshold activities has often left it blindsided.

Actors

It is very difficult to discern Russian narratives from homegrown Polish narratives, and Ukraine is a case in point. Hard-right politicians from the Konfederacja and Korona Polska, as well as elderly post-communist left-wing politicians such as former prime minister Leszek Miller and the journalist Monika Jaruzelska, happily engage in anti-Ukrainian rhetoric. Grzegorz Braun and the people he surrounds himself with, most recently, the Fire Extinguisher Front (Front Gaśnicowy), are the most committed promoters of narratives that serve the Russian cause. His open letter to Russian Foreign Minister Sergey Lavrov about the poor state of Polish–Russian relations could be seen as a performative act, but it is symptomatic of a climate conducive to malign information campaigns.

This is not to say that the public space has been void of pro-Russian elements. Przemysław Witkowski, one of the most prominent Polish researchers of the radical right, has called this the "partia rosyjska" (Russia party). After 1945, the communist government and the Marxists supported Russia, but from 1986, pro-Russian sentiment was more common among nationalist, ultra-conservative and ultra-religious groups (e.g. Myśl Polska, Kamraci, wRealu and All-Polish Youth).

It is very difficult to pinpoint Russia's role and link Pro-Russian narratives to the Kremlin. The major email leak from the political operators Sargis Mirzakhanyan and Aleksander Usovsky in 2014-2017 is one of the few publicly available pieces of evidence. It shed a lot of light on the way these operations are funded. As a result, some Russians were expelled from Poland. However, as technology advances and cryptocurrencies flourish, mapping these channels from Russia to Poland has become even more complicated. More rapid technological development means more rapid disinformation and manipulation. Moreover, Polish political operators have become more adept and tread carefully, avoiding any traceable connections to Russia.

Channels

The erosion of trust in the state and any relevant authorities, be it medicine, public intellectuals or the media, has emboldened Russia. Twitter, now known as X, has historically been the platform where conspiracy theories, hate speech and verbal aggression spread most easily. Poland has traditionally had a high proportion of its population on the platform, making it an important space for political statements and direct communication. While Meta's platforms have traditionally been more restrictive, since 2025, the number of pro-Russian narratives has increased, particularly in Facebook groups. TikTok has also emerged as a conducive space for radical and emotional narratives that fit the patterns of Russian disinformation. As some researchers note, deficiencies in data transparency on major platforms make it more difficult to clearly identify inauthentic accounts run by foreign actors. See, for example, research published by the Atlantic Council's Digital Forensic Research Lab (DFRLab).

Long-form commentaries should, in theory, moderate opinions and ease emotions, but have become a repository for all kinds of narratives, both democratic discussions and pro-Russian manipulations. A considerable proportion of fake and partially true discussions has migrated to YouTube channels where, in the name of diversity of opinion and the struggle against presumed censorship, a wide range of fringe actors can become closer to the mainstream.

Narratives

Ukraine

The major Russia's narrative in Poland is scepticism towards Ukraine. Ukraine has been the cornerstone of Polish political thinking in the twentieth century. Be it Jerzy Giedroyc or Zbigniew Brzezinski, Ukraine was seen as fundamental to Polish security and a bulwark against Russian imperialism. Ukraine has been so important to Poland, and there are so many Polish–Ukrainian interactions, that external actors have done their best to exploit any tensions that appeared between Poles and Ukrainians or Poland and Ukraine. Since 2014, this has become a constant stream of disinformation and manipulation. Russia's full-scale war against Ukraine has led to the usual fatigue seen in societies, but the second half of 2025 saw a stark increase in cases of anti-Ukrainian narratives online (Demagog, Res Futura and others). Furthermore, the police have noted a steep increase in verbal and physical aggression against Ukrainians during 2025.

The history of World War 2 (WWII) and the Ukrainian nationalist massacres of Poles are central to bilateral relations, and they have a long history of manipulation by the communist Polish state, the Soviet Union and Russia. Furthermore, the independent states have shown little goodwill in resolving this very painful chapter of their shared history. Researchers and civil society have been vocal in stressing the risks of unresolved historical questions being exploited by malign foreign actors, of which Russia is the most active.

The mass migration of Ukrainians to Poland after the start of the war in 2014 led to multiple examples of malign influence campaigns. Politically, neither Ukraine nor Poland did much to defuse the tensions. Until recently, Ukraine refused to allow the large-scale exhumation of murdered Poles, while the promotion at the national level of the WWII Ukrainian Insurgent Army (UPA) provided ample space for manipulation. Cases of monuments to victims destroyed by unidentified perpetrators were followed by failed investigations on both sides. Poland's failed law from 2018 banning symbols of "Ukrainian nationalism" sowed further divisions. These historical tensions have been deftly exploited by foreign actors, with social media enabling the rapid transmission of anti-Ukrainian sentiment. By 2025, even the fringe concept of "Banderite ideology" (Pol. ideologia banderizmu) had entered the political mainstream.

However, 2025 saw a massive increase in anti-Ukrainian sentiment. While there has been some natural discontent and frustration in Polish society, both Polish politicians and external actors have contributed to deepening these divisions. Anti-war sentiment, with the slogan "to nie nasza wojna" ("this is not our war"), has become a heavily trending phrase online. Russia's drone attack against Poland on 9 and 10 September 2025 was complemented by a large-scale online disinformation campaign, with almost 40% of the comments on Polish-language social media profiles attributing the blame to Ukraine. A few days later, there was an uptick of comments online claiming that Ukraine and some Polish politicians were dragging Poland into a war. While Ukraine received the most blame, Poland's Foreign Minister Radoslaw Sikorski, known for his unwavering criticism of Russia and ironic comments about its leadership, came a close second (see Res Futura and the subsequent discussion with the Institute for Media Monitoring). This was occurring in parallel with Russian state media propaganda pushing the argument that the drones were Ukrainian and that the overinvested Polish military was seeking to drag the West into a war with Russia.

Even the blatant case of the bombing of Polish railways by Russian agents did not lead to outright condemnation but created nuanced discussion on the far right, with certain voices blaming Ukraine for dragging Poland into the war or simply manipulating information regarding the citizenship of the bomber (see Ewa Wojciechowska-Hernik's comments). The recent decisions by the Polish govern-

ment to support arms purchases and collective borrowing for Ukraine at the European Union (EU) level have met with waves of criticism, and the radical right is continuing to build its financial arguments against what it claims is Poland's unconditional support for Ukraine (see December 2025 statements by Konfederacja).

Other prominent Ukraine-related narratives involve **refugees and migrants**. After Russia's full-scale invasion of Ukraine, Polish solidarity was extraordinary, but the society was under strain. One narrative involved Ukrainian men working in Poland rather than serving in the army. Just as men were criticised for avoiding military service, female Ukrainian refugees were portrayed as stealing Polish men from Polish women. As early as May 2022, reports were being made to the police of anti-Ukrainian hate speech (see Racist and Xenophobic Behaviour Monitoring Centre). As the war dragged on, new frictions arose and were escalated on social media and by national politicians, always treading a thin line between domestically fake news and outside interference. After the 2014 occupation of Crimea, Ukrainians were predominantly economically disadvantaged migrants who took on a variety of menial jobs. However, as refugees from all strata of Ukrainian society arrived in Poland following Russia's full-scale invasion of Ukraine in 2022, this created new tensions that could be easily exploited. Social media platforms were full of comments, genuine or fabricated, about Ukrainians showing off their wealth or being ungrateful.

These tensions did not ease as Ukraine became a key issue in the 2023 parliamentary election. The import of Ukrainian grain into the EU and its transit through Poland stirred some of the most negative emotions, particularly among farmers from regions where anti-Ukrainian sentiment has always been more prevalent and where the immediate threat from Ukrainian competition was greatest. The public's attention was captured by a tractor driver with a Soviet flag and a poster asking Putin to take care of Ukraine, Brussels and the Polish government. While no cases of direct Russian interference have surfaced to date, many people in the EU and even more in Ukraine perceived this as a blatant case of Russian activity.

The issue of "**gratitude**" would come to dominate the discourse on Polish–Ukrainian relations during 2025, with the President, Karol Nawrocki, serving as the opinion leader. Amplified by anti-Ukrainian accounts (and individuals from America's "alt-right" movement), throughout 2025 these narratives developed in new directions, such as Ukrainian greed, extortion of Western funds and an unwillingness to negotiate a peace deal. The decision by the liberal Civic Platform candidate Rafal Trzaskowski in January 2025 to provide social support for refugee children only served to normalise the scepticism among the general population.

The Russian use of Ukrainian citizens as disposable agents has helped to drive a wedge between Poles and Ukrainians. According to publicly available data, Ukrainian citizens (also from occupied territories) comprise the largest number of people charged with sabotage. This has been easily exploited on social media to promote fake news, such as Ukraine dragging Poland into the war, while supposedly blaming Russia. This narrative has been pushed by Polish politicians such as Ewa Hernik-Zajączkowska and amplified on social media.

Polarisation and the Reliability of the Polish State

The Polish political scene has become notoriously polarised, with few signs of improved cohesion in the near future (see Sierakowski & Sadura, Ekiert). This "Polish-on-Polish war", as it is often described by political commentators, has provided fertile ground for the weakening of state institutions. The Smolensk air disaster in 2010 marked a rift in Polish society that would only deepen over the years. The Russians did not miss the opportunity to exploit this (see Grzegorz Rzeczkowski).

The courts and the state media have been central to political divisions. In Poland, trust in the legal system is among the lowest in the EU, and the legal reforms introduced by the Law and Justice government post-2015 have further eroded trust (Eurobarometer, CBOŚ). This distrust is regularly fostered on social media, where claims of politically motivated privileges are common. Prominent cases, such as Judge Tomasz Szmidt fleeing to Belarus, were just one more hit to the image of state institutions. The military and border guards became one of the most polarising topics between 2021 and 2023 (this time, it was the liberals who were undermining state institutions), with the liberal camp radicalising narrative. Russia and Belarus instrumentalised the migration crisis and exacerbated it by waging an information war against Poland. Polish politicians were eager to exploit images, creating opportunities for Russian disinformation campaigns to portray Polish soldiers and officials as needlessly cruel, on the one hand, and incapable of protecting the border, on the other. Russia and Belarus also exploited the same narrative of Polish rule-breaking.

Occasionally, Russia would also launch direct information attacks, such as the generally unsuccessful attempt to create panic by sending false text messages with information about mobilisation. In 2024, a cyberattack on the Polish Press Agency (PAP) resulted in two fake publications about the mobilisation of 200,000 civilians destined for military service in Ukraine.

Following the drone attack, Russia promoted narratives portraying the incident as a fabrication by Polish insti-

tutions, thereby casting doubt on the state's ability to respond. Similar arguments are observed and have been more extensively studied in cases such as the COVID-19 pandemic and the controversy surrounding Poland's abortion ban. The women's rights issue has been examined in greatest depth by activists such as Klementyna Suchanow, who identified specific Russian actors contributing to these divisions. Meanwhile, the COVID-19 pandemic and related medical disinformation were recognised in 2024 by a Polish state commission as areas of potential Russian activity, although it stopped short of establishing clear connections to Russia. By 2025, a new fault line of division relating to Ukraine appears to have emerged, with liberals tending to advocate unequivocal support, whereas conservative and more radical anti-system parties are increasingly voicing discontent.

Sovereignty and Poland's Place in the World

The overall themes of isolationism and sovereignty have been central in narratives complementary to Russia's strategic goals. The fall of Western civilisation has been a popular trope for Russia's propaganda operations across the world, and Poland is probably not an exception. For Polish radicals, the restoration of independence has been a major slogan. It usually means the severance of ties with the EU, the rejection of the special security arrangements with the US and a general distrust of Poland's neighbours. It is in Russia's interest to amplify distrust in international organisations and allies, even while supporting Poland's huge defence investment to suggest Poland is "going it alone".

Historically, Poland has been one of the most pro-EU countries in the EU. However, when looking more closely, it is easy to identify times when that support has wavered. The past three years have marked a period of constant decline, almost reaching levels seen in 2004–2005. As of 2025, already around 25% of sceptical of the EU, be it positive sentiments, benefits or membership overall. Between 2015 and 2023, the Polish government was in a permanent conflict with the EU over the rule of law. At the same time, prominent European politicians were supportive of Donald Tusk and the liberal opposition parties. In an already polarised society, this caused an even stronger turn away from the European mainstream. Researchers have also claimed that Polish pro-European sentiment is very shallow, with economic arguments playing the greatest role. Now, as Poland is nearing the EU average and life quality has improved the citizens are losing their pro-European credentials. The issue of adopting the euro has repeatedly stirred the public imagination, with fears of lost sovereignty and unelected officials dictating Poland's economic development.

Russia has been identified as the disseminator of disinformation by the EU (Council conclusions), but local actors have also played a role. Again, Grzegorz Braun has been the epitome of anti-European sentiment, building on a long tradition of euroscepticism at the political fringes. The phrase "eurokołhoz" has been central to his political identity. He regularly compares the EU to the Soviet Union and claims that Poland had more freedom as the Russian-ruled Kingdom of Poland in the nineteenth century.

Polish–American relations have historically been viewed very positively in Poland, reaching 80% in 2023, but since Donald Trump's election, this fell to just over 30% in 2025. This may be seen as nothing special, given the controversial politics of the US president, but just as with any other division, this decline could be exploited by Russia. In the long term, there is the image of Poland as an American puppet state, losing its hard-won independence. Narratives about the unreliability of American equipment, the exploitative relationship with the US and the puppeteering in Russia's war against Ukraine have all appeared on Polish-language social media. The antisemitism of the Polish far-right has also been fertile ground for anti-American narratives. Due to America's central role in NATO, this also spills over into the anti-NATO sentiment that has, in general, been much weaker in Poland than across many other European nations. However, Russia has been consistent in creating doubts about NATO's commitment and reliability (see DisInfo Radar). This plays well with the narrative of treachery by the West in failing to defend Poland in 1939. While it has been used by prominent historians, it is a potent narrative for anti-Western sentiment.

An alarming dynamic can also be observed in **Polish–German** relations. Over the past century, these have been very difficult, and even the improvement after 1989 now seems like a short-lived moment. The German state has failed to see the process of reconciliation as a long-term commitment and to recognise that the explicit murder of Poles during WWII was something that would come to haunt the partnership at the centre of European politics and economy. The Polish right wing has exploited this ruthlessly, creating an opening for Russian actors to boost the tensions and distrust on both sides. Russia-friendly German politicians, mainly from the far-right party Alternative für Deutschland (AfD), have used this opportunity to sour Polish–German relations with comments about the Germans not being responsible for the destruction of Poland in the twentieth century and Poles being the "Afro-Americans of Europe" with their postcolonial mentality (see COMPACT-Geschichte, Aleksandra Gauland or Fabian Keubel).

One more recent development is not directly linked to Russia but has carved out its own niche in recent years. This is the left narrative that has arisen as a result of the Israel–Palestine war that has been ongoing since 2023. This has seen an attempt to relativise Russian crimes

against Ukrainians, putting them into a global context and presenting them as nothing special or a case of **Western double-standards** (see Mościcki). While the progressive left is a minor political force in Poland, this distrust of Western alliances and the international order that Poland has benefited from is a trend to watch.

Reactions

The rise in anti-Ukrainian sentiment, euroscepticism and polarisation, combined with the consistent improvements in the fortunes of political parties peddling Russian narratives, points to a lack of political will, failures by state institutions and the sheer scale of malign information campaigns. A Russia that refrains from creating new narratives but exploits existing tensions in Poland and amplifies them is extremely difficult to tackle. The spectre of censorship in a politically heated environment can be paralysing. These narratives are propagated by Polish citizens, and the legal system is slow to put a stop to hate speech and the spread of false information. While subthreshold attacks on infrastructure require significant planning from the Russian side and are easy to trace, low-intensity informational activities can be disseminated at a very low cost.

Russian media channels were never popular in Poland and were permanently banned by the Polish state in 2022. The disintegration of the traditional media landscape and the polarisation in media only accelerated the erosion of trust. Therefore, the focus of troll factories and similar entities has been the social media platforms where Poles get their information (very strong among the 18–44 cohort and which is well above the EU average). Fortunately, as with Russian TV channels, Telegram did not really take off in Poland and is mostly used by foreign-language speakers and foreign actors seeking disposable agents, as well as for criminal activities, rather than spreading narratives among the Polish population.

At the forefront of the fight with online fraud, disinformation and election interference is NASK, Poland's state research and development institution responsible for keeping the internet safe for everyone and protecting users from digital threats. While helping state institutions become resilient in the face of direct cyberattacks is its primary task (Poland is among the most attacked countries in the world), research into and advice on disinformation is also high on its list of priorities. Another important institution capable of responding rapidly is the Government Centre for Security (RCB), which has DisInfo Radar and a text-message alert system. The Polish Ministry of Foreign Affairs has changed its structure to include the Department for Strategic Communication and Countering Foreign Disinformation and established the advisory Council for Resilience, which includes many recognised experts. The Council published its recommendations for the government in December 2025. The focus was on the state administration taking on a larger role in tackling malign influence and better coordination between ministries and various state agencies. It recommended greater financial support for civil society initiatives but left a strong sense that these are insufficient given the scale of the problem.

Polish attempts to create a special state commission to investigate Russia's influence on internal security could have been seen as an excellent initiative, but the polarised environment meant that its sole aim was to incriminate political opponents. The first commission was established by the Law and Justice Party shortly before the 2023 October parliamentary election, which led to a change in government. The brief report published after the election advised against entrusting Donald Tusk, Bartłomiej Sienkiewicz or Tomasz Siemoniak with any functions related to state security. Leaving the scant evidence aside, it targeted the politicians who were to become, in just a few weeks, the prime minister, the minister responsible for special services and the minister of culture.

The commission was relaunched in 2024 to investigate Russian disinformation activities. Its report, published in January 2025, was much more balanced, highlighting some of the narratives mentioned above. It also focused on the shortcomings of the Polish state, stressing the need to supplement its analytical capacities with units working to counter disinformation. General expert opinion favoured more preventive or pre-emptive measures over real-time debunking. Pre-bunking domestically created false narratives has a high political price. One option floated by the expert community involved saturating the information space with content produced by trusted sources or generated with AI tools based on Polish-language sources, such as the Polish Large Language Model (see PLLuM by the Polish Academy of Science).

Polish military officials, initially behind closed doors and more recently on social media, have been more vocal in highlighting Polish–Ukrainian relations as the most vulnerable aspect of Polish defence. The murder of an eleven-year-old by a twelve-year-old in southern Poland in December 2025 prompted a statement put out by the General Staff of the Polish Armed Forces, stressing that claims about the killer's Ukrainian origins were a case of Russian disinformation. Considering that not all that long ago, giving the nationality of suspects or offenders in press articles and official statements was seen as stigmatising migrants, this marks a significant change in strategy. It also continues a pattern of communication by the General Staff, with regular posts on Facebook about Russian disinformation and influence campaigns, particularly against Ukrainians. Considering the high level of trust the military enjoys, this engagement is extremely useful.

Polish state think tanks, such as the Centre for Eastern Studies, the Mieroszewski Centre and the Narutowicz Institute, have been very good at identifying threats and raising public awareness about them. However, they have been very cautious when challenging politicians or even academics about their dissemination of Russian narratives. In some specific cases, "strategic silence" may be the correct choice, even if it means ignoring some of the more extreme narratives.

One European response to disinformation and greater control of social media platforms was the Digital Services Act (DSA). However, for some groups in a polarised society, the DSA came to represent censorship from an unelected European bureaucracy. When vetoing the national implementation of the DSA, President Karol Nawrocki compared the proposed Polish law to George Orwell's 1984. The rejection of international solutions might have also been influenced by the close alliance between Donald Trump's administration, Karol Nawrocki, and the wider Law and Justice political camp. With the American administration staunchly against European regulation of American companies, there seems to be a dead end. The general distrust of the European bureaucracy among parts of the polarised Polish society makes the entire subject even more problematic. An additional solution may be to share best practices with other partners, such as Ukraine, which is already being implemented at the agency level.

Looking at the overall picture, the impression is that Polish civil society has been at the forefront of defending the state against Russian narratives. Here, there is the usual risk of falling into the trap of polarisation, as civil society is usually seen as better aligned with the political centre. These include the European Research Collective Res Futura, the Media Monitoring Institute (IMM), Foundation INFO Ops, the Association NEVER AGAIN and the Association Demagog. They use AI-based tools to monitor internet traffic and track trends. Independent analysts, such as Anna Mierzyńska and Ludwik Rey, carry out important work informing the Polish public about any threats, and they are resolute in naming names. From 2025, Polish state companies, which include some of the biggest businesses in Poland (see PZU, PKO BP), are using its foundations to support these civic initiatives with actual funding.

However, the scale of the problem seems beyond the capacity of even the most carefully implemented individual initiatives. This is particularly true of key decisions that should be taken at an international or supranational level. The traditional slogan of "more education" might not be enough. Some seed initiatives, such as the scheme to support local media and local opinion leaders (see Ministry of Culture and National Heritage) might be a small step in the right direction.

Conclusions

Russia's interference in Polish discourse is certain, but the exact scale and intensity are incredibly difficult to measure. There are spikes in targeted activity, but most of the time, pro-Russian actors or direct Russian agents simply peddle disinformation and narratives created by Poles themselves. This undermines trust in state institutions and supports Polish isolationism or a narrow definition of sovereignty. Over the past year, however, the anti-Ukrainian narrative has come to dominate the Polish information sphere. Ukrainians are blamed for unresolved historical issues and accused of greed and warmongering.

Polish state institutions are now, more than ever, aware of the risks posed by malign and false narratives, but they have been slow to translate their excellent analytical capacity into positive action. State institutions tread a thin line between freedom and censorship in democratic societies and must be careful not to cross it. The legal framework is slow to react to the fast-changing media environment. The scale of the problem has forced the military and other, less politicised parts of the state apparatus to take the initiative. The current information space requires a large amount of content, and those who are pro-democracy must have the means of supplying it.

Under these conditions, it is Polish civil society that plays a leading role. Its ability to move faster and more directly is very important. However, the question remains whether, in the face of the information war, it is enough to rely solely on civil society.

Conclusion

Donata Ketlerytė

Project Manager at the Geopolitics and Security Studies Center

Shared Threat Landscape

The analysis of eight countries of the Baltic Sea region – Lithuania, Latvia, Estonia, Finland, Sweden, Denmark, Germany, and Poland – demonstrates that, despite differing national contexts, all countries face a common adversary in the realm of propaganda and disinformation: Russia, and its similar but contextually tailored tactics. While some countries also experience information operations originating from other actors, such as neighbouring Belarus or more distant China, the primary source of disinformation targeting the Baltic Sea region remains Russia.

The Baltic Sea region is exposed to a wide range of Russia's information operations. These activities are primarily carried out through social media (particularly platforms such as Telegram, TikTok, and YouTube) as well as traditional media. Increasingly, a broad set of tools is employed beyond disinformation, including AI-generated content, deepfakes, manipulated video material, forgeries, the distribution of fake emails, cyberattacks, hack-and-leak operations, espionage, phishing, narrative repetition, and cloned media websites.

Information operations are relatively low cost for Russia, enabling them to be conducted rapidly, frequently, and at scale across the region. Notably, Russian information campaigns frequently rely on strong emotional framing, aiming to amplify their impact and more effectively influence public perceptions and behaviour in the societies of the Baltic Sea region countries. Recently, these informational campaigns are becoming increasingly sophisticated and are often accompanied by broader hybrid activities by Russia.

Differing National Contexts and Vulnerabilities

An important observation is that the countries in the Baltic Sea region differ significantly in their national contexts. Some states, such as the Baltic countries, which were occupied and annexed by the Soviet Union for a prolonged period, share a border with Russia, and have Russian minorities (around 5% in Lithuania, over 20% in Estonia, and 25% in Latvia), which contributes to the political instrumentalization of Russian-speaking minorities and shapes country-specific narratives employed by Russia.

Others, such as Sweden and Finland has recently experienced increased pressure from Russia particularly in relation to NATO-related issues. Meanwhile, for Denmark, Russian information operations represent a relatively recent development. For a long time, Denmark was not a primary target of Russian information campaigns; however, this is increasingly changing. Notably, Denmark stands out within the region, as information campaigns tend to focus more on shaping perceptions about Denmark internationally. At the same time, while operating within Denmark's information space, Russia also engages with geopolitical aspects of Denmark's domestic agenda, particularly the question of Greenland. In contrast, in both Poland and Germany, disinformation is strongly centred on Ukraine: in Poland, they primarily target the presence of Ukrainian refugees, seeking to exploit societal tensions, while in Germany, Russia's efforts focus on weakening public support for Ukraine, constraining Europe's ability to mount a coordinated response.

Particular attention should be given to the case of Finland. Despite receiving sustained attention in Russian media between 2000 and 2024 (the highest among the Nordic countries), Finland remains among the most resilient countries in the region to (Russian) disinformation. This resilience can be attributed to a strong domestic consensus on foreign policy, as well as a relatively small Russian-speaking minority, notwithstanding Finland's shared border with Russia.

Main Russian Narratives and Strategic Objectives

It can be observed that all countries in the Baltic Sea region are confronted with the same hostile actor, which conducts information campaigns across each of them. At the same time, Russia's primary objective remains consistent throughout the region: to weaken societies, fragment political consensus, and undermine the reputation of the EU, the United States, and NATO among domestic audiences. Accordingly, both the narratives promoted and the tools employed by Russia are broadly similar across the countries of the Baltic Sea Region.

COUNTRY	THEMES TARGETED BY THE DISINFORMATION	MAIN CHANNELS	STRATEGIC OBJECTIVE
Lithuania	Erosion of trust in Lithuanian institutions; The West and Western governance; The war in Ukraine; The portrayal of the Russian regime as stable and efficient; Geopolitical reordering and the "new world order"; Migration and refugees as instruments of influence; The revival of Litvinism.	Social and traditional media.	Undermining institutional trust and societal cohesion.
Latvia	The revival of Nazism; Alleged preparation for war against Russia by Latvia and the West; The rights of non-citizens in Latvia; Latvia as a failed state; Nostalgia for life under the USSR.	Social and traditional media;	Sowing confusion and polarization, undermining societal resilience, and delegitimizing democratic institutions.
Estonia	The West and Western governance; The inevitability of escalation in the war in Ukraine; Rising prices linked to the war in Ukraine.	Social and traditional media, including source laundering, coordinated amplification, and the use of deepfakes.	Undermining trust, increasing polarization, inducing decision-making paralysis, and eroding confidence in state institutions.
Finland	Finland portrayed as sympathetic to Russia (in contrast to "nationalist" Baltic states); Western countries' ties with Russia; Refugees as a source of societal destabilization; Finland-Russia relations as natural partnerships despite tensions; The impact of sanctions on the EU versus Russia; NATO as a threat to Russia; Public support for NATO membership in Finland.	Social and traditional media.	Increasing distrust in Western institutions and NATO among Finnish citizens.
Sweden	The role of the United States in the war in Ukraine and the European energy crisis; The war in Ukraine; Alleged Swedish support for terrorism; Sweden's NATO membership as anti-Russian and externally driven; Societal decline in Sweden linked to immigration, crime, and moral decay; Sweden as a subordinate "vassal state" of the United States and NATO.	Social media, including Russian-language media outlets operating in Swedish, as well as coordinated forgeries and hack-and-leak operations.	Undermining support for NATO membership, increasing polarization around immigration, and eroding trust in Sweden's political and societal stability.

COUNTRY	THEMES TARGETED BY THE DISINFORMATION	MAIN CHANNELS	STRATEGIC OBJECTIVE
Denmark	The war in Ukraine; Denmark's geopolitical role, including Greenland.	Social media, including the use of manipulated audiovisual content, false news, and AI-generated materials	Shaping international perceptions of Denmark and influencing its image abroad, rather than directly targeting domestic audiences.
Germany	Russia portrayed as misunderstood rather than imperial; The effectiveness and societal impact of sanctions; The futility of Ukraine's defence; The risk of escalation due to increased Western support for Ukraine; Ukraine portrayed as corrupt and failing; Russia as a rational actor seeking peace.	Social media, supported by coordinated digital ecosystems.	Weakening German support for Ukraine, fragmenting political consensus, and undermining Europe's ability to respond collectively.
Poland	The war in Ukraine as unrelated to Poland's national interests; Ukraine as dragging Poland into the war; Alleged Polish territorial ambitions toward Lviv, Hrodna, and Vilnius; Anti-NATO sentiment; Ukrainian migration to Poland.	Social media.	Sowing doubt, discontent, and polarization, undermining European unity, and fostering tensions between Polish and Ukrainian communities

Key Recommendations for the Region

Taking into account the experiences of all eight countries highlighted in this publication, several key recommendations adaptable across the Baltic Sea region can be identified.

1. **Strengthening civil resilience, public education and media literacy:** sustained attention should be given to educating society to recognize disinformation across traditional and new media, maintain basic cybersecurity hygiene, and understand the origins and mechanisms of conspiracy theories. As highlighted across all countries examined in the publication, media literacy remains a fundamental component of resilience and requires continued investment from the governments. Media literacy should be systematically integrated into national education systems across the Baltic Sea region in a comprehensive manner. This includes not only students, but also broader segments of society, including teachers, journalists, and public servants.

2. **Increasing the security of media and information infrastructure:** countries in the region should allocate greater resources to strengthen existing media structures and their cybersecurity systems, addressing technological vulnerabilities, and continuing to implement measures to protect broader information infrastructure.

3. **The effective integration of the Russian-speaking minorities:** in several countries in the region (e.g. Latvia, Finland, Estonia, and Lithuania), Russian-speaking minorities are seen as one of the most vulnerable groups. Due to their consumption of Kremlin-aligned information channels (even though most countries have banned Kremlin-owned television channels) they remain among the instruments of Russian soft power. Strengthening alternative information channels that provide reliable content in the Russian language is therefore essential in order to reduce reliance on Russian-language news accessed via social media platforms (particularly channels such as Telegram, WhatsApp, TikTok, and others), where disinformation and pro-Kremlin narratives are actively disseminated. This should be accompanied by sustained efforts to improve the education system and further develop digital literacy skills among these minorities. At the same time, it is recommended to review the activities of Russian-linked institutions and community structures (such as Russian Orthodox churches affiliated

with the Moscow Patriarchate and "Russian Houses"), as these may serve as channels for the spread of disinformation. Furthermore, countries should review migration policies and consider more restrictive visa measures, alongside strengthened background checks for members of the Russian opposition residing in the countries of the region, while continuing to support those actors who are assessed as credible and aligned with democratic values.

4. Faster reaction: strengthening the early warning and analytical capabilities: Russian disinformation and propaganda campaigns are characterized by their speed and wide reach. Accordingly, countries in the region must adapt their responses by developing effective monitoring systems, establishing clear response protocols, and ensuring timely information-sharing among institutions and with partner countries - an aspect particularly relevant in the context of the Baltic Sea region. As highlighted throughout the publication, monitoring systems should be further developed to move beyond simple fact-checking of content and instead focus on identifying how disinformation is disseminated by hostile actors. This includes shifting from purely reactive debunking to incorporating prebunking approaches that anticipate and mitigate future disinformation narratives. States should also possess the tools and capacities to effectively disrupt disinformation campaigns, including, where appropriate, the blocking of networks and coordinated activities, as well as the ability to respond rapidly with clear and credible communication to prevent societal fragmentation. In addition, crisis management exercises should incorporate disinformation scenarios, training institutions to manage the impact of such campaigns on public perception, behaviour, and decision-making.

5. Strengthening the transparent strategic communication: Transparent strategic state communication is a cornerstone of strengthening a country's ability to withstand disinformation campaigns conducted by hostile actors. In this regard, countries in the region should: 1) enhance their strategic communication capacities by communicating proactively, clearly identifying hostile actors, and maintaining consistency in messaging; 2) ensure transparency in communication in order to counter narratives promoted by Russia that portray truth as unattainable. State communication should be as open as possible, and when faced with information gaps or the inability to disclose certain details, authorities should clearly acknowledge these limitations and, where necessary, admit communication mistakes; 3) protect critical institutions and academic freedom, while promoting investigative journalism practices in order to ensure a more secure and trustworthy information environment.

6. Adapting the legal and institutional frameworks to the digital and hybrid threat environment: legal frameworks and regulatory measures in the region should function in close coordination with other instruments in countering disinformation. States should seek to adapt legal regulation to the realities of the new media environment, with particular attention to social media platforms. This includes the development of clear reporting mechanisms, strengthened cooperation with platform representatives, and the establishment of effective tools and response protocols to limit the spread of hostile information once identified. At the same time, legal and institutional frameworks should strengthen cross-sectoral cooperation, as disinformation campaigns often evolve into broader hybrid activities conducted by hostile states, especially Russia. It is therefore essential to establish and maintain mechanisms capable of identifying linkages between informational, logistical, and kinetic actions, enabling a more comprehensive and timely response.

7. Strengthening international communication: Countries such as Lithuania, Denmark, and Sweden highlight that Russian disinformation campaigns target not only domestic audiences but also shape international perceptions by promoting distorted narratives about these countries. Greater emphasis should therefore be placed on clear and consistent communication in English, strengthening countries' democratic narratives abroad and national positions in the international arena. Other countries in the Baltic Sea region should anticipate similar challenges, as Russian disinformation tactics are often replicated across the contexts of different countries. Governments should ensure the capacity and tools to monitor, analyse, and respond to such campaigns when necessary.

References

1. Statistika, Tautinių mažumų departamentas prie Lietuvos Respublikos Vyriausybės <https://tmde.lrv.lt/lt/tautiniu-mazumu-kulturos-centrai-ir-tautines-bendrijos/statistika/>

2. RV067: POPULATION BY ETHNIC NATIONALITY AND SEX, 1 JANUARY, Statistics Estonia <https://andmed.stat.ee/en/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV067>

3. Russians in Latvia, Minority Rights Group <https://minorityrights.org/communities/russians-4/>

GSSC

GEOPOLITICS AND SECURITY STUDIES CENTER