

**EESC**

Eastern Europe  
Studies Centre  
Established in 2006

# Index of Russia's Influence on Lithuania 2022–2023

Tomas Janeliūnas





**Tomas Janeliūnas** – Head of Research Programmes, Centre for East European Studies, Professor at Vilnius University Institute of International Relations and Political Science.

## Summary

- Following Russia's invasion of Ukraine on 24 February 2022, Lithuania has taken active steps to reduce its dependence on Russia. The biggest changes have taken place in the economic, energy and information domains, where the links with Russia or the potential influence of Russian entities on Lithuania have been minimised. However, the obvious reduction in Russia's possible influence on Lithuania does not mean that Russia has completely disappeared from our security, economic, energy, political, or information environment.
- The Index of Russia's Influence on Lithuania, which has been conducted for the first time, is based on a survey methodology published in 2022. The study covers seven domains involved in the state's functioning – military, economic, energy, cyber, information, political and societal security – where the factual connections and, consequently, the spread of Russia's potential influence on Lithuania through these linkages were assessed. In total, the index used 27 categories of criteria.
- The value of Russia's potential influence on Lithuania in 2022-2023 measured 3.13 on a 10-point index scale (where 1 means no tangible influence and 10 means the maximum possible influence).
- According to expert surveys, Russia's greatest potential influence is in the cyber domain, with an average score of 5.5. This level of influence is mainly due to Russia's ability to exploit various software and hardware security vulnerabilities in Lithuania and the potential to carry out targeted cyber-attacks and other malicious activities against Lithuania's critical IT and communications infrastructure. The experts also pointed out that, on average, more than half of all cyber incidents targeting Lithuania could be attributed to Russian entities.

- The domains of societal security (3.6 out of 10 possible points) and politics (3.4 points) scored slightly higher marks than the final average value of the index. In the domain of societal security, Russia has the potential to substantially impact Lithuania due to the relatively passive political-social nature of Lithuanian society. On the other hand, Lithuanians reject the typical Russian propaganda narratives and demonstrate a strong understanding of and support for the principles necessary for democracy.
- In the political domain, the main negative impact is due to the high distrust of key governmental institutions among the Lithuanian society. The low trust in political institutions is perhaps the most vulnerable point in terms of political security: people's lack of trust in the authorities undermines the strength of the society's connection to the state. On the other hand, the position of the Lithuanian parliamentary parties is completely against Russian political interests, and the popularity of radical parties in the national political system is minimal. However, this trend may change – the 2024 elections in Lithuania should reveal whether public support for radical views has increased.
- The military (2.4), economic (2.2) and information (2.2) domains scored lower than the overall index average. The results indicate that these domains are more immune to Russia's influence, which is mainly due to the restrictions or policy decisions introduced after February 2022, ranging from the almost complete refusal to import Russian energy sources to the sharp drop in the turnover of goods and services with Russia, to legal decisions banning the availability of Russian information sources in Lithuania.
- The study is based on aggregated statistical data for 2022-2023 and surveys conducted with experts in their fields. There was no clear quantitative data in some assessment categories or such data gathering would be highly inefficient, so subjective expert judgements were used. It is worth noting that despite the subjectivity of the expert assessment, it often reflects the assessments of independent experts or researchers and the generalised assessments of institutions (e.g., the Ministry of National Defence, the State Security Department and the National Cyber Security Centre).

## Introduction

For Lithuania, 2022 was the year of the 'great disengagement' from Russia: the war in Ukraine prompted a severe reduction in almost all formal ties. The EU economic sanctions against Russia and Russian counter-sanctions have reduced the trade volumes and encouraged businesses to withdraw from the Russian market. Furthermore, Russia's energy blackmail, which started as early as 2021, has prompted a clear rejection of any energy import from Russia: Lithuania announced in [May 2022](#) that it would be the first EU country to stop buying Russian gas, oil and electricity. The Lithuanian communication regulators and law enforcement authorities started blocking Russian-sponsored propaganda channels on the internet and TV broadcasts. Thus, Russia's already limited influence on Lithuania seems to have been completely neutralised.

However, the obvious reduction in Russia's possible influence on Lithuania does not mean that Russia has completely disappeared from our economic, energy, political or information domains. Some Lithuanian businesses are still unable to get rid of their companies operating in Russia. Clever use of the sanctions loopholes is helping businesses find new ways around them and continue trading with Russia. Even after the officially declared 'energy disconnection', we are still part of the BRELL electricity transmission circuit, controlled by Russia, and some Russian energy products (i.e. gas) continue to enter or transit through Lithuania. Furthermore, after the initial blockages, some Russian propaganda sources continued to be available to Lithuanian users without much difficulty. While Russia's ability to influence has been diminished, this may only be temporary. It is difficult to guarantee that, in the long term, the Russian regime – unless it changes fundamentally – will abandon its intention to regain or strengthen its influence over countries it has long regarded as its 'near abroad' or in Russia's sphere of influence.

This study is the first attempt to comprehensively assess Russia's influence on Lithuania and identify the areas where Russia's influence may still pose significant risks and threats. Periodic 'fact-checking' will allow us to monitor how the factual situation is evolving and will help to highlight the most sensitive areas.

It should be noted that this study does not seek to assess the *threats* posed by Russia. This function is performed by the National Security Department and the Second Department of Operational Services, which annually provide an overall assessment of the threats to Lithuania's national security.

As discussed in more detail in the 2022 Methodological Guidelines on Russia's Influence on Lithuania (in Lithuanian only), *influence* can take many forms, ranging from coercion through hard power to persuasion through soft power or attractiveness. Having in mind the modern concept of *power* and *influence*, the Index of Russia's Influence on Lithuania is constructed according to the following assumptions:

1. Russia's overall influence includes 'hard', 'soft', and 'sharp' influences, which can affect Lithuania's security, economic, political, and information sectors and public attitude. The assumption is that both the form of the impact and the sectors of the impact are interrelated and that an impact in one sector can change the situation in another.
2. The scope of the potential influence is primarily determined by the objective *scale of the connections between Lithuania and Russia*: e.g. the volume of bilateral trade, the number and size of the audience of Russian propaganda channels operating in Lithuania, energy supply flows and infrastructure, and so on. The greater the extent of the various types of links between the two countries, the greater that impact can be.
3. The level of vulnerability creates the conditions for a successful *sharp* influence, but the effectiveness of such an influence can be captured by indicators reflecting the favourability to Russian goals (e.g. political decisions favourable to the Russian regime or the proportion of the population supporting Russian narratives). In many cases, this effectiveness can only be measured through expert knowledge or public opinion surveys.
4. The index should be based on effective criteria and data – particularly on a manageable amount of data and variables. Some of the criteria may be derived from objective data (e.g. volume of trade, number of energy infrastructure connections, summarised results of a public opinion poll), but some of the criteria will have to be formulated based on expert judgement due to the complexity of the criteria (and will therefore inevitably involve a degree of subjectivity).

The main function of this index is not to identify particular forms of influence, but to provide an overall picture and a basis for comparison.

The study is based on the 2022 Methodological Guidelines on Russia's Influence on Lithuania. These guidelines set out the principles and possible methods for assessing Russia's influence on Lithuania based on the best theoretical and applied examples of measuring power and influence. The index is constructed by assessing Russia's links and potential impact on seven areas of Lithuania's state functioning. In total, the index uses 27 categories of criteria, combining both quantitative data and qualitative expert judgements.

Many of the statistics include summarised data for 2022 (e.g. trade volumes, investment shares, etc.) or the latest available data for the actual situation in 2023. In cases where expert assessment have been used to calculate category-specific indices, it should be taken into consideration that the experts' comments were made in the context of the situation in the summer-autumn of 2023.

## Military domain

Index of the influence  
on the military domain

**2.4 out of 10**

The assessment of the potential influence on Lithuania's military domain was based on three categories: the extent of official military cooperation; the extent of Russian military supplies and their use in Lithuania; and the Russian military's intelligence capabilities in Lithuania. All of the categories were based on expert assessments provided by representatives of the Lithuanian Intelligence Service, the Ministry of National Defence and other officials working directly in the field of Lithuanian national security.

### Scope of Military Cooperation

Dependence on another country's military decisions may be based on existing formal agreements on bilateral cooperation, formal obligations under international treaties, and specific factual needs that require consideration of the other country's decisions or interests. Russia's potential influence expands as the links and scope of its military cooperation increase: the more joint or overlapping military structures and

agreements, the potentially greater Russia's influence will be. An example of a maximum level of military influence is the military integration between Russia and Belarus, where the Collective Security Treaty Organisation (CSTO) commitments on common defence, the provision of a common air defence system, and other bilateral agreements have effectively made Belarus completely dependent on the Russian military influence.

However, even between countries that see each other as enemies, there may be opportunities for cooperation or agreement. For example, such cooperative links may include Russia's membership and participation in international security institutions (e.g. the Organisation for Security and Co-operation in Europe (OSCE), the former NATO-Russia Council, UN Security Council, etc.), bilateral agreements on activities of a military nature (e.g. the Lithuania-Russia agreement on military transits to and from Kaliningrad), agreements on the provision of observers for regional military exercises, and exchanges of disarmament or arms control and surveillance missions.

As of 2022, Lithuania no longer maintained formal bilateral military cooperation relations with Russia. Lithuania also has no bilateral military cooperation agreement with Russia.

Previously, Lithuania's official commitments to inform or coordinate its decisions and actions with Russia in the military domain have been based on the so-called Vienna Document – the OSCE's agreement on the cooperation of its members under confidence and security-building mechanisms. The [Vienna Document](#), adopted in 2011, includes a commitment to inform the parties to the agreement about planned military exercises, plans to deploy weapons along their borders, periodic exchanges of military observer missions and other aspects. The Vienna Document agreement also includes the [Open Skies Treaty \(2002\)](#), which allows the parties to the agreement to conduct unarmed aerial reconnaissance flights over the territories of all other parties. According to the Vienna Document, military observer missions have been carried out between Lithuania and Russia in the past (most recently in 2015). However, security and confidence-building measures are currently suspended, and there are no military observer missions between Russia and Lithuania. In December 2021, Russia also formally withdrew from the Open Skies Treaty.

The transit of the Russian military through Lithuania was based on the 1993 Agreement between the governments of Lithuania and Russia, which stipulated

that military transits were to be carried out subject to permits and under the laws of Lithuania and international law. As most Lithuanian military experts have mentioned, the rules applicable to military transit were favourable to Lithuania, as they allowed the country's officials to obtain detailed information on the transportation of military personnel or equipment in the territory of Lithuania and, if necessary, to refrain from issuing permits. As of April 2022, Russian military transit through Lithuania has ceased. The cancelled military transit has reduced the risk of potential provocations and the potential impact of these on Lithuania's security.

However, some of the links and Russia's indirect ability to influence persist: e.g. the experts mentioned the obligation to coordinate overlapping communication frequencies with the Russian military structures that use the spectrum needed for 5G communication. Russian military equipment operates in the 5G band frequencies, so the Russian side argued that the frequencies intended for civilian use could interfere with Russian stations, which should be given prioritised protection. The decision in 2021 was unfavourable to Lithuania, which delayed the implementation of 5G tenders in Lithuania. After four years of disputes, only in the spring of 2023 did the International Telecommunications Union finally rule in favour of Lithuania.

Russia can also have an indirect influence through other Lithuanian allies, which may seek to return to arms control agreements or confidence-building mechanisms with Russia in the future. Russia is still a member of the OSCE and the UN Security Council. Thus, it indirectly influences the international security system and decisions that may affect Lithuania. The military transit agreement, which is still formally in force, maintains a minimal link in military cooperation, which can be used as a pretext for various political or disinformation claims against Lithuania.

## Scope of the Supply and Use of Military Equipment

If a foreign country supplies arms and other military equipment, its influence over the recipient increases. This is especially true for a smaller country, where the scale of the influence depends on the share of military supplies in the overall defence spending structure. An influence in this category can also potentially occur after the supply has ceased: mainte-

nance, spare parts, or the potential risk of exploiting known or secret vulnerabilities in military equipment (in particular, vulnerabilities in information systems, identification signals, etc.) can maintain the influence from the arms' country of origin.

Lithuania has no Russian arms or equipment supply contracts, and all of its weapons and military equipment are sourced from NATO countries or other reliable partners and allies. Until 2022, there may still have been some Soviet or Russian light weapons or ammunition left in the warehouses of the national defence system or other law enforcement agencies; however, since 2022, according to the experts, essentially all Soviet-time equipment has been donated to Ukraine. The only remnants of Russian-origin equipment are Mi-8 transport helicopters in the possession of the Lithuanian Air Force. For the operation of these helicopters, Lithuania is still dependent on spare parts from manufacturers linked to the Russian Federation. However, we do not buy them directly from Russian companies.

Although equipment or software of Russian origin may not be used directly by the armed forces or the national defence system, some other companies whose activities are linked to the military security of the state - e.g. transport (especially railways and airports) or information technology companies - may still be using some potentially vulnerable equipment. The Russian-origin equipment used in these strategic sectors can potentially pose risks to the national defence, from data collection to the initiation of potential diversions. For example, the procurement by Lithuanian Rail of a Russian-origin KLUB-U locomotive safety system, which may be based on the Russian Glonass satellite navigation system, has been the subject of separate investigations. This system has been considered unsafe and incompatible with Lithuania's national security system.

However, the experts said there are only very rare, isolated cases where companies that have won procurement contracts offer technologies of Russian origin or from Russia-associated companies. In recent years, the procurement requirements have been tightened. Previously, only transactions among strategic companies of national security importance were subject to inspection, but now, the transactions of critical information infrastructure managers are also being inspected. As of 2022, control over the procurement of goods and services in the national defence system has been tightened by introducing an internal procedure whereby important purchases are subject to investigation by the National Security

Department, the Second Investigation Department under the Ministry of National Defence and the General Prosecutor's Office.

Since 1 April 2023, the procedure for issuing import and export licences for strategic goods (military and/or dual-use equipment) has been strengthened. An additional criterion has been added, which may lead to the non-issuance of a licence – due to relationships with specific persons if this increases the risk or threatens Lithuania's national security.

## Russian Military Intelligence Capabilities in the Country

Suppose a hostile country has a significant intelligence presence in our country. In that case, the influence on our military capability, deterrence, potential defence and counter-resistance capabilities can be significantly increased. Intelligence tasks can range from gathering sensitive military data to acts of sabotage. In addition, active intelligence and recruitment activities can increase the risks of a hostile country gaining influence by recruiting high-ranking officials or politicians. The assumption is that the greater the intelligence capability, the greater such an influence can be.

It is important to distinguish between Russian intelligence's surveillance and passive information gathering capabilities – especially through signals (SIGINT), satellite surveillance and cyber means (CYBERINT) – and its human intelligence (HUMINT) and recruitment capabilities and its potential for penetration of the national defence system of Lithuania. In the first case, Lithuania's proximity to the heavily-militarised Kaliningrad and Belarus, whose intelligence services cooperate very closely with Russian military intelligence institutions, means that Lithuania cannot, in principle, be shielded from Russia's ability to observe and collect data on Lithuania's armed forces and military capabilities.

According to Lithuanian intelligence authorities, Russia uses stationary and mobile platforms for signals intelligence (SIGINT) in the Kaliningrad region and other parts of Russia, as well as in Belarus, to carry out surveillance tasks for Russian intelligence needs. Commercial, passenger and research vessels registered in Russia can conduct intelligence activities in the Baltic Sea. Information on the military and civilian

infrastructure is also gathered by cyber means while penetrating the systems of governmental institutions and analysing the data available in open sources.

The Russian intelligence services are especially active in Lithuania's border regions. Thus, Lithuanian citizens travelling to Russia or Belarus remain at high risk. According to the Lithuanian intelligence officers, Russian intelligence is regularly interested in people living in Lithuania who visit relatives in Russia or Belarus. The Russian intelligence services are almost certain to collect and systemise information on all persons travelling to these countries and assess their ability to gather information in Lithuania, their favourability towards the Russian and Belarusian regimes, and their possible vulnerabilities or weaknesses. This activity implies the intention to recruit such persons actively. By August 2023, the flow of Lithuanians to Belarus alone remained extremely high, reaching around 230 thousand border crossings in the first six months of 2023. Such high traffic creates favourable opportunities for Russian and Belarusian intelligence services to select potential recruitment targets.

On the other hand, according to Lithuanian intelligence services, Russia's ability to conduct human intelligence against Lithuania has been reduced. In 2022, five officials of the Russian Federation working under diplomatic cover were expelled from Lithuania. In addition, the sanctions imposed on Russia, restricting travel by Russian citizens to Lithuania, have also reduced the ability of Russians working with Russian intelligence agencies to visit Lithuania.

Lithuania's national defence system has no documented cases of high-ranking officials cooperating with Russian or Belarusian intelligence services. In principle, this may reflect the relatively high level of resilience of the Lithuanian military and intelligence system and the effective work of the counter-intelligence and immunity units. However, the penetration of Russian intelligence services into the intelligence services of NATO countries has been documented on several occasions and is an ongoing concern. Therefore, the vulnerability of Lithuania's national defence system may depend not only on the resilience of the Lithuanian institutions but also on the resilience of other NATO allies. As a result, some of the experts interviewed increased their scores because of Lithuania's dependence on the potential vulnerability of its allies or international organisations, caused by the intense Russian espionage during recent decades.

Index of the influence on the military domain	2.4 out of 10
Average of the expert assessment (on a scale from 1 to 10, where 1 is no influence at all and 10 is the maximum dependence on Russia)	
Scope of military cooperation	1.8
Scope of the supply from Russia and use of military equipment in Lithuania	2
Russian military intelligence capabilities in Lithuania	3.4

## Economic Domain

Index of the influence on the economic domain	2.2 out of 10
---	---------------

The Lithuanian economy is heavily dependent on foreign trade. As a small country, Lithuania needs to be open to foreign trade, and the growth of the Lithuanian economy as a whole depends to a large extent on the development of the export industry. In 2022, Lithuania's foreign trade (goods and services) to GDP ratio was 177%, one of the highest in the EU.

Lithuania's foreign trade with Russia has long accounted for a significant share of Lithuania's total foreign trade. In 2021, Russia was Lithuania's largest export partner, accounting for 10.8% of the country's total exports. Russia also ranked 2nd after Germany in imports, accounting for 12.1% of Lithuania's total imports. Mineral fuels have traditionally accounted for the majority of the country's imports from Russia.

In 2022, the foreign trade flows to and from Russia dropped significantly, amounting to EUR 5.32 billion, 36% lower than in 2021. Correspondingly, exports to Russia contracted 27% to EUR 2.73 billion, while imports were 43% lower at EUR 2.6 billion. **Russia's share in total foreign trade (excluding services – EUR 96.6 billion) was 5.5% in 2022**. Accordingly, Russia dropped to 5th place in the list of Lithuania's most important foreign trade partners.

There are various methodological interpretations of when a state's dependence on a foreign trading partner can become dangerous, and consequently, the economic impact of such a dependence can become a major security vulnerability. Economists have no consensus on additional criteria such as export concentration, overall level of trade diversification, etc. However, there is a recurrent assessment that

a 30% or more share of foreign trade may lead to a significant dependence on the export market or the country of origin of those imports. In today's world, most countries seek to diversify their foreign trade, recognising that a heavy dependence on another country's imports or exports creates significant economic and political tension. However, in some cases, extreme levels of trade dependence are recorded; for example, in 2021, Belarusian exports to Russia amounted to 45.7%, while imports to Russia were 54.5% of the total volume of the corresponding trade.

The transformation of the foreign trade dependency ratio into a 10-point system assumes that a share of 30% or more in foreign trade would imply a very high degree of dependency and influence, i.e. it would be worth 10 points. Accordingly, 1 point means a share of less than 3% of foreign trade; 2 points means a share of 3-6%; 3 points means a share of 6-9%; and so on. **The 2022 foreign trade data shows that Lithuania's trade with Russia can be converted to 2.8 points.**

The Lithuanian statistics present exports and imports of services separately from imports and exports of goods. According to data from the Bank of Lithuania, in 2022, the total services exports amounted to EUR 17.4 billion, and imports amounted to EUR 11.4 billion. The value of services provided by Lithuanian businesses in Russia in 2022 amounted to EUR 655 million, or 3.8% of the total service exports, while imports from Russia amounted to EUR 322 million, or 2.8% of the total imported services. **The total turnover of services with Russia amounted to 3.4%** of Lithuania's total services received and rendered with foreign entities, which converts to **2.2 points**.

As with the trade in goods, the flow of services to and from Russia has decreased: in 2021, EUR 788 million worth of services were exported to Russia and EUR 532 million worth of services were imported. On the other hand, there is a trend of a declining turnover in services, although it is not consistent: in Q1 2023, Lithuania exported about 36% fewer services than in Q1 2022, while the volume of services received from Russia dropped by 80%. Transport services accounted for a dominant share of the Lithuanian exports.

However, there is an important point to bear in mind: while the volume of direct trade in goods and services with Russia has dropped since 2022, there has been a significant increase in the flow of goods and services with third countries (Kazakhstan, Armenia, Georgia, etc.), which are helping Russia to circumvent the trade sanctions imposed on them.



**Figure 1.** Imports and exports of services to Russia in 2022-2023



Source: Bank of Lithuania, Exports and imports of services by country in 2023.

## Share of Foreign Investments

Russia has long been one of the most important investors in Lithuania, although Lithuanian companies were cautious about doing business in Russia even before the military aggression in Ukraine in 2022. According to [the data of the Bank of Lithuania](#), in Q1 2023, the total direct investment (FDI) accumulated in Lithuania amounted to EUR 31.7 billion, while Lithuania's accumulated FDI abroad reached EUR 13 billion. The Russian FDI in Lithuania in Q1 2023 amounted to EUR 323 million (**1% of the total FDI in Lithuania**), while Lithuanian investments in Russia amounted to EUR 158.6 million (**1.22% of Lithuania's total investments abroad**).

Accordingly, these **FDI indicators can be transformed into a score of 1.1** on a ten-point scale to assess Lithuania's dependence on Russian foreign investments and the flow of Lithuanian capital to Russia.

Although the total amount of Lithuanian investment in Russia is relatively small, it is worth noting that despite the war in Ukraine, Lithuanian capital has not been substantially withdrawn from Russia in recent years. In fact, quite the opposite is true: while the cumulative investment balances in Russia amounted to EUR 130.7 million in Q1 2020, EUR 112.3 million in Q1 2021 and EUR 130.7 million in Q1 2022, they reached EUR 158.6 million in Q1 2023 – the highest level in the last few years.

According to a [survey by Verslo žinios](#), in 2023, more than 140 Lithuanian-owned companies were operating in Russia. According to the Russian register of legal data, the largest revenues in Russia in 2022 were earned by manufacturing, trade, transport and other companies owned by Visvaldas Matijošaitis and his business partner Liudas Skierus (whose shareholders are either Vičiūnų grupė or VG Holding) – the revenues of these 8 Lithuanian companies amounted to about EUR 368 million, and the net profit amounted to EUR 37.86 million.

The reluctance of the Vičiūnų grupė to leave Russia has become the most prominent example of how a small number of Lithuanian businesses have not given up their intention to work in Russia, which can result in their vulnerability. The case of Vičiūnų grupė is also special because its *de facto* leader, Visvaldas Matijošaitis, is also a politician of significant importance as he is the Mayor of Kaunas City. In individual cases, this intertwining of business and politics could significantly increase Russia's influence through specific Lithuanian politicians who remain vulnerable because of their investment in Russia.

## Dependence of Strategically Important Sectors of the Lithuanian Economy on Russia

Representatives of major Lithuanian business associations and chief economists of Lithuanian commercial banks were asked to assess the remaining dependence on Russia in strategically important sectors of the economy. Lithuania's strategic economic sectors are energy, finance, transport, and IT and communications.

The subjective ratings ranged from 1 to 5, with an **overall average expert rating of 2.8**.

Almost all the experts stressed that Lithuanian businesses currently have, essentially, only trade relations with Russia. According to the experts, there are no significant investment and technological contacts, and Lithuania does not receive any strategic raw materials. As one expert put it, 'First, the Covid-19 pandemic seriously altered the supply chains, and the war in Ukraine has now almost completely disrupted the chains with Russia. Compared to other EU countries, we are probably the least dependent on that country.'

According to the experts, the Lithuanian financial system is almost completely isolated from Russia, with almost no communication. Some experts stressed that 'the only tangible dependence remains in the energy sector' and that this is because Lithuania's electricity grids are still part of the 'BRELL circuit'.

However, it was also mentioned that some small road transport companies still depend on the Russian market. Although Russia's influence on the transport sector as a whole has been significantly reduced (as is reflected in the decline in the turnover of Lietuvos Geležinkeliai and the Port of Klaipėda), some experts have singled out the transport sector, which may be influenced by Russia, in particular when trying to reach the countries of Central Asia or China via rail. However, the association representatives additionally pointed out that 'signals' from transport companies indicating their vulnerability to the Russian market have also decreased.

Index of the influence on the economic domain	2.2 out of 10
Trade in goods with Russia as a share of Lithuania's total exports and imports	2.8
Trade in services with Russia as a share of Lithuania's total exports and imports	2.2
Share of Foreign Investments	1.1
Dependence of Strategically Important Sectors of the Lithuanian Economy on Russia	2.8

## Energy Domain

**Index of the influence on the energy domain**  
**2.6 out of 10**

Energy security is traditionally defined as the continued ability of a country to ensure the availability and accessibility of its energy resources in ways and at prices acceptable to society. These elements of energy security include the ability to have access to energy resources or to import them from other countries without hindrance (availability), the uninterrupted transmission of energy through internal and external channels and infrastructure (accessibility), the support of the public, the choice of what type of energy should be developed, and the affordability of energy prices that are acceptable to businesses and other consumers (affordability).

Lithuania's energy sector has been particularly dependent on Russia for a long time due to a limited infrastructure capacity to secure energy resources through alternative import routes. However, after the launch of the LNG terminal (in late 2014) and the construction of electricity interconnections with Sweden and Poland (in 2016), Lithuania has significantly improved its energy security, at least in terms of infrastructure (availability and accessibility).

However, even after securing access to other countries' oil, gas and electricity, the trade in Russia's energy resources has remained very intense. In 2020, according to Eurostat data, Lithuania had one of the highest levels of energy import dependence, at 74.9% (the EU average was 57.5%). The situation was even more depressing when looking at the dependence on Russian imports in relation to the country's total gross available energy consumption: the figure was as high as 96.1% in 2020 (mainly due to imports of Russian oil, which is refined at Mažeikių nafta, while a large part of the oil products produced was exported).

However, since the spring of 2022, measures have been taken to replace Russian gas, coal, oil and electricity with imports from other countries. Some of these decisions were taken by businesses (e.g. PKN Orlen announced in the spring of 2022 that it would no longer use Russian oil in Mažeikių nafta), and some decisions were linked to economic sanctions imposed by the EU and the US on Russian banks (e.g. Nord Pool, the operator of the electricity exchange, decided in May 2022 to halt the trading of Russian electricity from Inter RAO, the sole impor-

**Table 1.** Share of imports from Russia in Lithuania's total energy consumption for 2020

	Total	Natural gas	Oil	Coal
European Union (27 countries)	24.4%	41.1%	36.5%	19.3%
Lithuania	96.1%	50.5%	202.7%	69.1%

Source: Eurostat, [https://ec.europa.eu/eurostat/statistics-explained/images/2/24/EnergyMixDependencyImports\\_25-03-2022.xlsx](https://ec.europa.eu/eurostat/statistics-explained/images/2/24/EnergyMixDependencyImports_25-03-2022.xlsx)

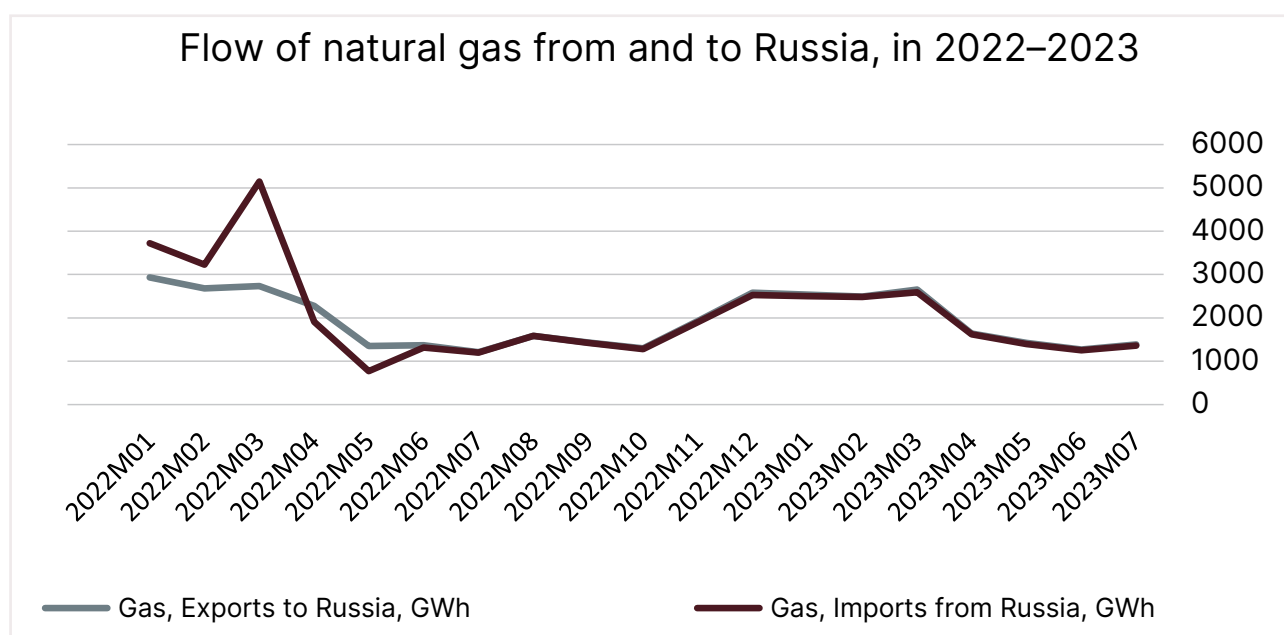
ter of Russian electricity in the Baltic States). This became a pretext for the [Ministry of Energy of the Republic of Lithuania to announce](#) that from 21 May 2022, Lithuania would no longer import oil, gas and electricity from Russia.

Technically, however, this is not entirely true. The energy flows from Russia have not been completely cut off. Formally, imports of electricity and gas from Russia are still recorded. However, almost all of it is exported to the Kaliningrad region, i.e. there is actually a transit of gas and, to a very small extent, a transit of electricity or balancing of the technical flows. According to Lithuanian statistics, the actual imports of crude oil from Russia stopped in April 2022 (1.4 million tonnes were imported in the first three months of 2022), and August 2022 was the last month Russian coal was imported to Lithuania. Electricity imports have been almost non-existent since

May 2022 (while in the first five months of 2022, 754 GWh of electricity was imported from Russia). However, Lithuania continues to import liquefied petroleum gas from Russia, with 40.5 thousand tonnes of liquefied petroleum gas (mostly used for transport) imported to Lithuania in the period of January to July 2023. Furthermore, this flow has increased compared to the period up to February 2022, as this energy resource is not included on the sanctions list. On the other hand, liquefied petroleum gas accounts for an insignificant share of the overall energy balance, so this change cannot have any real impact on Lithuania's dependence on Russia.

Gas trade with Russia, although taking place on the principle of transit, still suggests that Russia retains an influence in this area. By comparing the actual gas trade data for January to July 2023, it can be seen that 13,209 GWh of gas (or 38.3% of Lithuania's

**Fig. 2** Imports and exports of natural gas to Russia, 2022-2023



Source: Lithuanian Statistics Portal, Fuel and energy imports and exports

total natural gas imports) was imported from Russia, and 13,408 GWh (or 52.2% of Lithuania's total natural gas exports) was exported. The actual gas trade with Russia, while not directly affecting Lithuania's energy needs, has the potential to become a pretext for political pressure. Similarly to the transit of other goods to Kaliningrad, which caused a lot of tension in mid-2022, Russia's influence in the gas sector remains, notably through Lithuania's indirect commitment to ensuring gas transit to Kaliningrad. The gas transit through Lithuania also puts a strain on Lithuania's gas infrastructure, which requires appropriate maintenance and servicing (throughout 2022, 64 TWh of gas was transported through the Lithuanian gas transmission system operated by Amber Grid, of which about 23 TWh, or about 36%, was intended for transit to the Kaliningrad region).

Considering that the gas trade with Russia accounted for about 45% of the total gas trade turnover (imports+exports) in the first half of 2023, Russia's impact on Lithuania's gas trade volumes can be assessed at 4.5 points.

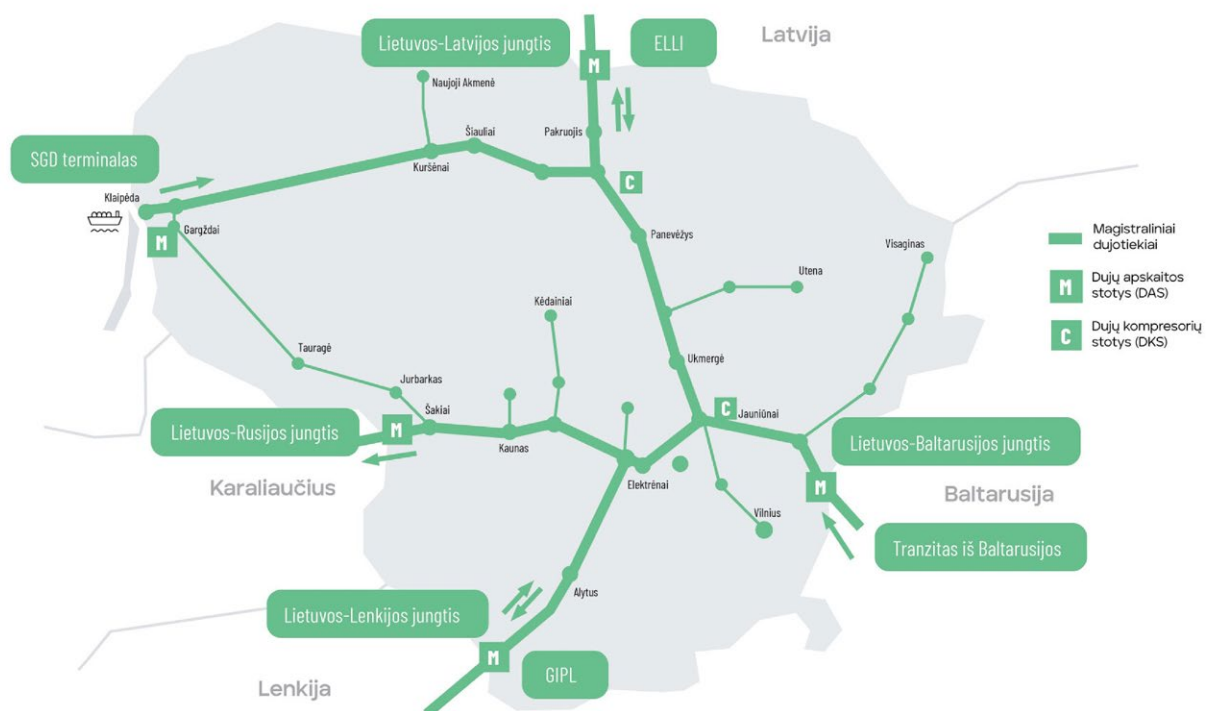
On the other hand, these links can be seen as a process of mutual dependence – Kaliningrad's gas supply is still largely dependent on Lithuania's transit, while Russia's exclave's electricity generation is

also secured by gas combustion, so Lithuania has a potential leverage point if, for example, Russia decides to unilaterally disconnect the Baltics from the IPS/UPS system.

There is no formal trading in the electricity sector, but there are electricity exchanges to support the system's needs. However, the figures for electricity imports and exports are small: imports from Russia in January to July 2023 amounted to 18 GWh (0.3% of the total electricity imports), while exports amounted to 95 GWh (or 5% of Lithuania's total electricity exports). Russia's share in the total electricity trade was only 1.5%. Accordingly, the persistence of trade with Russia in the electricity sector results in a score of 0.2 points.

Trade in the oil sector is no longer taking place, with Mažeikių nafta having already switched to supplies from other countries last year. No oil products are being supplied to Russia either. On the other hand, considering the small volumes of oil product imports from Russia, the energy sector's dependence on Russia is 0.1.

**The overall average score for the energy sector's dependence on Russia in terms of the trade volumes, is 1.6.**



**Fig. 3** Map of the Lithuanian gas transmission system. Source: ambergrid.lt

## Energy Infrastructure and Entities with Links to Russia

Lithuania has come a long way in developing alternatives to Russia's energy infrastructure and moving away from the influence of Russian energy companies. One of the most important changes took place back in 2014 when the EU's third energy directive package was finally implemented, the gas supply, transport and distribution companies were separated, and Gazprom's shares in Lietuvos dujos were bought out by the Lithuanian state. The LNG terminal has allowed the country to import gas from outside Russia for the first time since the end of 2014.

However, for quite a long time, Russian energy companies had a significant influence on the Lithuanian energy market, ranging from the direct ownership of energy facilities (e.g. Gazprom held 99.5% of Kauno termofikacinė elektrinė until 2012), to a significant market share in the electricity sector – as late as in the second half of 2021, the wholesale electricity market was still dominated by InterRAO Lietuva (61.6% of all electricity sales on the wholesale market, and around 12% of the retail market). Although InterRAO Lietuva is formally majority-owned by the Finnish company RAO Nordic OY, the Russian electricity producer INTER RAO UES controlled the latter.

Lithuania is still linked to Russia in terms of its energy infrastructure connections. Two of the five inter-

connectors (or entry/exit points) in the gas pipeline system depend on Russia: the Lithuanian-Belarusian interconnector, which carries gas for the Kaliningrad region, and the Lithuanian-Russian interconnector.

In 2023, the electricity system was left with two 330 kV lines actually in operation out of the five former lines leading to Belarus, and two 330 kV lines out of the former three remain with the Kaliningrad region. There are also two 400 kV links to Poland and a 300 kV link to Sweden. The Lithuanian electricity system still operates in the IPS/UPS system (BRELL circuit), where the electricity frequency is centrally regulated in Russia. As many energy experts have pointed out, the functioning of the Lithuanian electricity system in the BRELL circuit is the last remaining serious sign of Lithuania's dependence on Russia. A connection to the continental European grids and synchronous operations with Poland and other continental European countries is planned for 2025.

Although the targeted disconnection of Lithuania (all Baltic countries) from the BRELL circuit is still mentioned as a potential threat from Russia, it should not significantly destabilise the Lithuanian electricity system. In April 2023, the system operator Litgrid carried out an isolated operation test, disconnecting Lithuania's electricity grid from the Russian-controlled IPS/UPS system, which confirmed Lithuania's capability to ensure the system's stable operation. On the other hand, if a disconnection from the IPS/

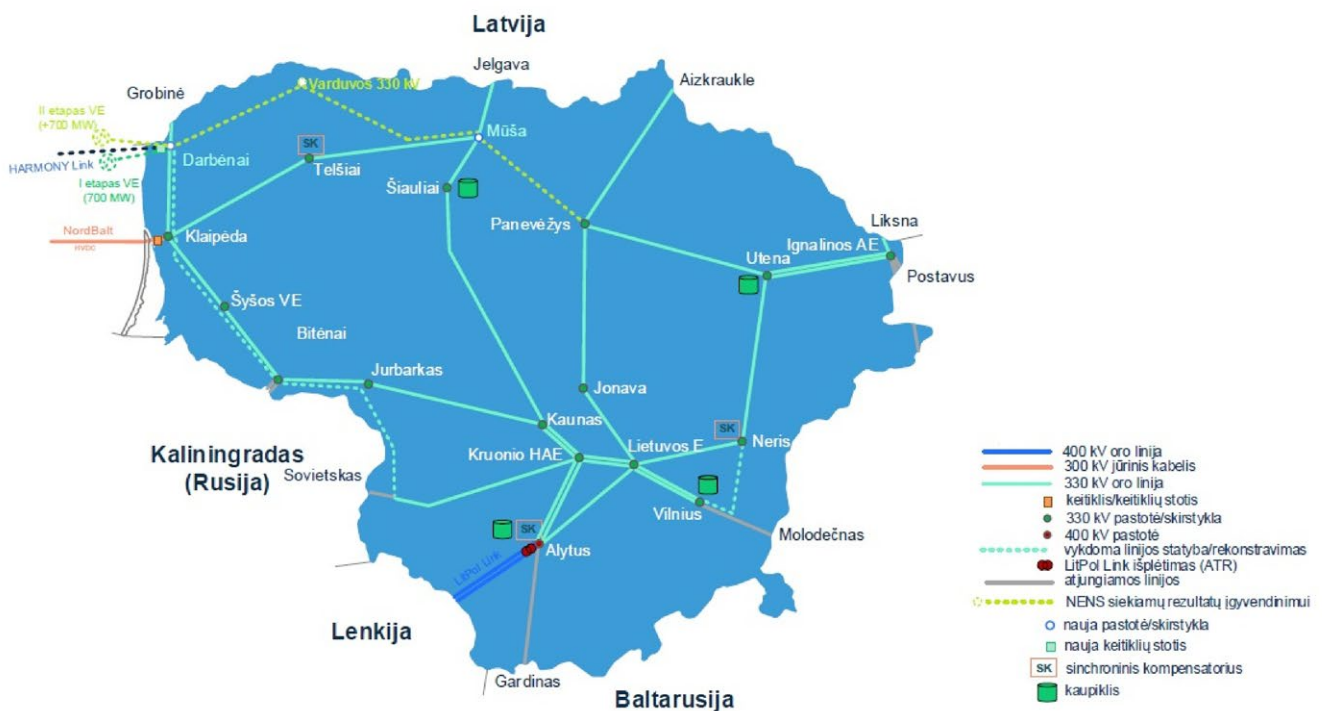


Fig. 4 Map of the Lithuanian electricity system and connections. Source: Litgrid.eu

UPS system were to take place before Lithuania, Latvia, and Estonia have completed their synchronisation with continental Europe, the stable operation of the system may require the switching on of 'expensive' generating facilities, which would significantly increase electricity prices in the region.

The cessation of commercial trade in oil, electricity and gas with Russia has significantly changed Russia's ability to influence the Lithuanian energy market through Russian companies and their representatives. With Lithuania's refusal to import natural gas and electricity from Russia, energy brokers have also lost their position and market share in Lithuania. Although some of them still maintain contacts in Russia, they have no influence on the energy market in Lithuania. As some energy experts noted, Lithuania has also seen cases where those wishing to invest in renewable energy have contacts with Russian entities. Still, Lithuania's legal framework provides opportunities to prevent risky or threatening investments. However, it has been observed that Russian entities try to participate in strategically important Lithuanian projects using third parties without disclosing their links. As was mentioned by the experts, some contractors, subcontractors, and suppliers of Lithuania's essential infrastructure construction and modernisation projects may be wholly or partly, directly or indirectly controlled by Russian entities. Thus, additional monitoring of threats of this nature (under the Law on Protection of Objects Critical for National Security) requires additional attention and resources from the developers of the projects, which often increases the costs and budgets and increases the timeframe for a project's implementation. On the other hand, as the experts said, within a year, procurement teams have had time to evaluate 1) the available pool of solutions and equipment, 2) the alternatives on the market for the required tools and devices, and 3) the development of action plans – from replacing Russian equipment to alternatives on the market with a reliable country of origin.

The **average score of the surveyed energy experts was 3.8** when summarising their assessment of Russia's influence on Lithuania's energy infrastructure and entities.

## Exposure of the Energy Policy to Russia's Influence

Russia's habits and capacity to influence the policies of its energy-dependent states, particularly by further deepening its energy dependence, has been

documented in numerous studies, official research and academic papers. The means of influencing another country's energy policy direction or specific decisions range from mild pressure to choose cheaper Russian resources to overtly corrupt or even violent actions. Lithuania's recent history also includes cases where Russia's influence on Lithuanian politics and decision-making has been exercised through various business entities. The best-known and most widely documented cases, which have led to parliamentary investigations or even impeachment of members of the Seimas, are the allegedly corrupt connections of Dujotekana with Lithuanian government representatives. These matters were discussed in 2007 in the material disclosed by the Seimas Committee on National Security and Defence from the Department of State Security, as well as in the impeachment proceedings against Mindaugas Bastys, who was also accused of protecting the interests of the [Russian company Rosatom in Lithuania](#), which were launched in 2017.

The scandalous stories from recent decades and Lithuania's declining energy dependence on Russia have significantly reduced the opportunities for Russian actors to influence Lithuania's energy policy decisions. As most energy experts noted, a direct influence on Lithuanian politicians has almost disappeared. The energy sector, especially when it comes to state-owned companies or associations, is striving for greater transparency, while the changing geopolitical situation has reinforced the need for stringent operational, stakeholder management and screening policies in energy organisations.

On the other hand, the experts pointed out that several years ago, Russian entities, to influence Lithuania's energy policy decisions, chose to lobby through international organisations and institutions, e.g. on issues related to the trade of Russian electricity, the synchronisation of the Baltic States' electricity systems with the continental European grids and the prospects of cyber security. The Russian representatives have sought to exploit their links with energy trading intermediaries to achieve their objectives. The Russian entities are currently thought to have very limited lobbying opportunities, but they are unlikely to give up lobbying, which will mask their interests' representation.

Another vulnerable area is Russia's efforts to continue influencing energy policy decisions through propaganda and manipulating public opinion. For example, a common topic is that restricting energy supplies from Russia imposes a heavy financial burden and significantly impacts the health of EU economies.

According to the experts, the formal and informal influence of marginal parties and politicians, as well as part of the influenced media and social platforms, on public opinion can be indirectly used to influence political decisions. Such information attacks aim to hinder or compromise the transformation of energy self-sufficiency, usually under the pretext of achieving lower prices for the customers, with the real aim of preserving the dependence on electricity imports and imported fossil fuels.

In previous years, the LNG terminal was the main target of such misinformation. Now, the topics are changing, with some experts mentioning that information attacks could be aimed at compromising offshore wind farm projects or the transformation towards renewables, decarbonisation of the country or the liberalisation of energy markets in general.

**The average score of the experts' assessments of the current exposure of Lithuania's energy policy to Russian influence was 2.5.**

Index of the influence on the energy domain	2.6 out of 10
Energy trade volume	1.6
Energy infrastructure and entities with links to Russia <i>(average of the expert assessment)</i>	3.8
Exposure of the energy policy to Russia's Influence <i>(average of the expert assessment)</i>	2.5

## Cyber Domain



### Opportunities for Russian Entities to Exploit Vulnerabilities in the Hardware and Software of Lithuanian Users

Cybersecurity and the attention to potential cyber vulnerabilities are gradually increasing for Lithuanian public institutions and businesses, as well as individual consumers. In recent years, there have been a number of cybersecurity simulations and training

sessions, with a particular focus on reducing the cyber vulnerability of critical infrastructure. However, the experts noted that the opportunities to exploit vulnerabilities in software or hardware, especially when accessing data, remain very high. It is also clear that Russian entities are actively exploiting these security loopholes – data collection can be caused by insecurity in hardware (e.g. internet routers), vulnerabilities in software (not necessarily of a Russian origin), or unknown features that allow for the collection of user data.

As an example of software insecurity, an [analysis](#) by the National Cyber Security Centre (NCSC) in 2019 revealed how the D-Link router and switch settings enable the routing and storage of the users' data in Russia's Yandex.DNS and SkyDNS systems. Although it is impossible to obtain precise data on the number of potentially insecure hardware or components used in Lithuania, according to cybersecurity experts, the problem remains very sensitive. Although the security vulnerabilities are constantly being checked, their extent is not precisely known. More recently, the increasing use of the Internet of Things, 5G equipment and a multitude of software add-ons to basic applications have increased this potential dependency and vulnerability. In addition, the experts noted that the use of Internet Protocol Television (IPTV) in Lithuania has expanded significantly in recent years, often by installing unreliable or 'hacked' applications. According to the experts, software piracy remains high in Lithuania, with a significant amount of illegal software coming from Russian sources. In many cases, such software has Trojan horses implanted, which the cybercriminals will exploit sooner or later. Mobile apps that fall into the 'grey area' are particularly difficult to control as their true origin is unclear, there is no clear guidance from the internet service providers or public authorities on whether they are safe to use, and it is unclear where the data is stored on physical servers. Among these applications, the experts most often mentioned 'plug-ins' or add-ons related to Yandex, Kaspersky or Viber applications. It is important to note that, according to Russian law, IT companies are obliged to keep their data servers in Russia, allowing Russian law enforcement and intelligence agencies easier access to the data they collect.

In summary, the cybersecurity expert survey, in which Russian entities were asked to assess the ability of Russian entities to exploit vulnerabilities in the hardware and software of Lithuanian users, yielded an **average score of 7.6** on the subjective assessment of the ability of Russian entities to exploit vulnerabilities to software and hardware.

## Dependence of Lithuanian State Institutions and Businesses on Software or Hardware of Russian Origin

For a long time, private or business users and official institutions have paid little attention to which software vendors they use and what security risks they face. While Russian-origin applications and apps have never dominated the most popular software categories, software with specific features may be prevalent in particular sectors. In addition, for a long time, Russian-origin software has had the advantage of cheaper licence prices than Western-origin alternatives. As a result, it is not uncommon to find Russian-origin software, even in public institutions, whose licences are still valid because they were purchased several years ago. For example, in 2018, the Bank of Lithuania acquired [C1 Company software](#) licences, which were due to expire in 2021. In particular, the form-filling software developed by ABBY was widespread in Lithuanian institutions: it was used for many years by the State Tax Inspectorate, State Social Insurance Fund Board, Customs Department and other institutions.

Among the most frequently mentioned software of Russian origin, or with links to Russian entities, were the *Kaspersky* anti-virus software, *ABBY* form-filling system, the document management and accounting applications *1C-Organizacija*, and the content management system *1C-Bitrix*. Although cybersecurity experts noted that critical infrastructure companies are largely free of Russian software products, some state organisations or businesses may still use popular Russian-origin applications or wait for them to expire/update. 'Usually, when licences expire, businesses and government organisations alike are trying to switch to Western software,' said a National Cyber Security Centre representative.

**The cybersecurity expert surveys, taken together, yielded an average score of 3.6** on their subjective assessment of how much Russian software Lithuanian users may still have in use. It should be noted that such software is already rare in state institutions, but the experts pointed out that businesses are not in a hurry to get rid of these risky applications once and for all.

## Russia's Ability to Conduct Malicious Activities Against Lithuania's Critical IT and Communications Infrastructure

In October 2023, [two incidents](#) were recorded in which data cables connecting Estonia to Finland and Sweden were damaged (the gas pipeline between Estonia and Finland was also damaged). Although the initial investigations focused on a Chinese commercial vessel, these incidents have raised significant concerns for NATO and have increased the need to strengthen the physical protection of the critical infrastructure at sea.

Lithuania has not yet experienced similar incidents of physically targeted damage to its IT and communications infrastructure. However, the experts pointed out that Russia knows quite well which infrastructure elements, cables or data processing centres are critical for the functioning of Lithuanian cyber services. Recent public data shows that Russian intelligence and military structures have devoted considerable attention to monitoring the energy and communications infrastructure and its potential vulnerabilities – especially at sea, where it is more difficult to ensure constant monitoring of the facilities (e.g. cables) or to detect destructive activities. Although the Lithuanian cyber security experts emphasised that it is unlikely to be possible to completely 'disconnect' Lithuania from the outside world (primarily because Lithuania has a fairly well-diversified network), there is still a risk of temporary disruptions in the provision of internet services.

Destructive activities such as disrupting internet services, hacking into non-public data systems or taking control of websites happen all the time – it is essentially a permanent low-intensity cyber war. The experts noted that state and business institutions are improving their skills to counter cyber-attacks, but some Lithuanian entities still lack training in this area.

There were no major changes in the Lithuanian cyberspace after the military invasion of Ukraine on 24 February 2022. According to the 2022 National Cybersecurity Report, the number of recorded cyber incidents (around 4 thousand) has remained similar to that in 2021. However, in some cases, particularly massive attacks have been recorded. For example, at the end of June 2022, the NCSC recorded a massive wave of DDoS attacks against the public and private sectors. Information on attempts to affect at least 137 publicly accessible websites was collected from public sources. A pro-Russian Federation group of hackers claimed responsibility for these attacks. In July 2022, Ignitis Group announced that it had suffered its worst



cyber-attack in a decade. ESO's website has been blocked, and Kill-net, a group linked to Russian intelligence, claimed responsibility for the cyber attack.

In 2023, the number of cyber incidents increased ahead of the NATO Summit in Vilnius. The NCSC estimates that the number of cyber-attacks occurring during the NATO Summit increased by up to 3 times. The IT systems of a Lithuanian regional radio station and the Panorama shopping centre were hacked, launching messages directed against NATO and the supply of arms to Ukraine. There were also quite massive DDoS attacks before and during the NATO Summit. Among those affected by these attacks were the websites of City Service, Akropolis, Orlen Lietuva, Linas Agro and Govilnius.lt, as well as the news agency BNS, 15min, alfa.lt and the m.Ticket services. Although it has not been made public, the cybersecurity experts said in the interviews that there were 'very serious attempts' to disrupt both air navigation systems and attacks on the country's critical infrastructure during the NATO Summit. However, these cyber-attacks were contained and did not affect the organisation of the NATO Summit.

One of the most unpleasant incidents related to the NATO Summit was the public [disclosure](#), after the Summit, of allegedly intercepted routes, timetables, and other security measures taken in Vilnius to plan and implement the guests' logistics. The data, consisting of at least 29 files, was shared by a group calling itself 'From Russia with Love'.

All of these incidents confirm that entities linked to the Russian government are constantly monitoring, capturing and actively exploiting cyberspace vulnerabilities to disrupt the delivery of IT and communication services. While these vulnerabilities could potentially be exploited not only by Russia, it is Russia's aggressive behaviour that is causing Lithuania the most trouble. Accordingly, this dependence on Russia belongs to the 'sharp influence' type, where a destructive influence is exercised. On the other hand, a large number of the potential cybersecurity vulnerabilities are like the invisible part of an iceberg under the water, and the cybersecurity experts stressed that in many cases, the incidents that have been recorded in Lithuania so far could be equated to 'testing' or verifying the level of vulnerability. **The overall score of the expert assessments of Russia's impact in this area was 7.7.**

## The Role of Russian Capital Companies or Related Companies in Lithuania's IT and Communication Services Sector

The Lithuanian IT and communications sector is dominated by Western capital companies (the largest are Telia, Bite and Tele2 in the data processing and internet servers segment; Hostinger in the communications equipment segment; Teltonika Networks, etc.). According to the experts' assessment, no significant Russian-owned or Russian-related companies are operating in the IT and communication services sector in Lithuania. On the other hand, some experts mentioned that individuals in prominent positions in large IT and communications companies had connections with Russia or Russian entities, at least in their backgrounds, and that there could potentially be some Russian influence channels. However, the impact of such individuals on the operations of the companies operating in Lithuania can only be assessed by intelligence services and is therefore not the focus of this study.

Russian-owned companies and Russian investors are not uncommon in Lithuania. One of the examples mentioned by the experts was Squalio Lietuva, a software trading company, the majority of whose turnover is made up of software licences from Microsoft, Cisco, Symantec and other companies (in 2022, Squalio Lietuva's [turnover](#) exceeded EUR 12 million euros). The Squalio group of companies (operating not only in Lithuania but also in Latvia, Estonia, Kazakhstan and Belarus) was acquired by Softline in 2021, a company linked to Russian investment and one of the largest software traders in Russia (in 2020, [the group's turnover amounted to about USD 2 billion](#)). In October 2022, Softline created a new brand, Noventiq, and launched an Initial Public Offering (IPO) on the London Stock Exchange. The main shareholder of Noventiq is the Russian businessman [Igor Borovikov](#). However, Noventiq could not technically be called a 'Russian company' (even though it was founded in Russia in 1993), as it has long been a multinational corporation.

When asked to assess Russia's potential influence through capital investments in Lithuania's IT and communications sector, the experts gave an **average score of 3.1.**

## Subjective Attribution of the Responsibility for Lithuanian Cyber Incidents to Russia

The responsibility (or attribution) issue in cyberspace is still one of the most complex issues in assessing cyber-attacks and the damage they cause. While it is technically possible to collect a large amount of data and eventually trace the perpetrators of attacks, it is still relatively rare for cyber attacks to be attributed to a specific state or public authority. This is often avoided for political reasons – if a state is found to have deliberately caused damage to the cyberinfrastructure or data, the issue of ‘punishment’ would have to be addressed. In political terms, this could potentially lead to a serious escalation. Therefore, in many cases, even if evidence is provided to show how public authorities are involved in the organisation of a cyber-attack, there is no follow-up to a legally or politically binding claim of responsibility.

Lithuania also has no formal record of legal proceedings directly targeting the Russian government or institutions for cyber-attacks. On the other hand, the experts were fairly unanimous in agreeing that a large number of cyber incidents, especially those that are not aimed at profiting but simply at disrupting the delivery of IT services, taking control of websites or spreading disinformation online, mostly originate in Russia (and in some cases China). According to the experts, the Russians (or hacking groups linked to Russia) often make little attempt to hide their intentions and publicly claim responsibility for data interceptions or other cyber incidents.

According to the experts’ general assessment, about 50% of the cyber incidents targeting Lithuanian state institutions or critical infrastructure can be attributed to a Russian origin. **The average score from experts in this sector was 5.2.**

Index of the influence on the cyber domain	5.5 out of 10
<i>Average of the expert assessment (on a scale from 1 to 10, where 1 is no influence at all and 10 is a maximum dependence on Russia)</i>	
Opportunities for Russian entities to exploit vulnerabilities in the hardware and software of Lithuanian users	7.6
Dependence of Lithuanian state institutions and businesses on software or hardware of Russian origin	3.6
Russia’s ability to conduct malicious activities against Lithuania’s critical IT and communications infrastructure	7.7
The role of Russian companies in Lithuania’s IT and communication services sector	3.1
Subjective attribution of the responsibility for Lithuanian cyber incidents to Russia	5.2

## Information Domain

Index of the impact on the information domain  
**2.2 out of 10**

### Russian Information Campaigns Against Lithuania

For a long time, Russia has been conducting targeted information operations and campaigns against Lithuania (and other countries) to discredit those countries institutions, including the benefits of Lithuania’s membership in the EU and NATO, individual Lithuanian politicians, and to increase public dissatisfaction with the government, or to promote public confrontation, the potential for protest and the tendency towards conspiracy theories. These information campaigns and operations are increasingly being carried out through unofficial channels, such as social media platforms (in particular, through fake accounts and targeting closed thematic groups) or websites, the origins of which are unclear and whose publicity is very limited. However, such campaigns and operations can impact particular groups in society, especially those who tend to distrust official information and public authorities.

The Strategic Communications Department of the Lithuanian Armed Forces (as well as other organisations such as Debunk.eu) monitors information attacks and records unique cases of disinformation. A unique case of disinformation is a primary, factual, original or other case of information dissemination that displays the characteristics of disinformation, manipulation, misinformation or another deceptive technique. This is one of the baseline indicators of the intensity of Russia’s information operations and campaigns. On the other hand, the number of unique cases alone is not enough to measure the reach of the audience, as the effect of sharing is also important.

In 2022, the Strategic Communications Department of the Lithuanian Armed Forces recorded 4,999 cases of unique disinformation. Furthermore, in the first ten months of 2023 (until 31 October 2023), 2,815 unique cases of hostile information activities were recorded. Nonetheless, there has been a trend for a steady decrease in the number of Rus-

sian and Belarusian disinformation incidents since July 2023, after the conclusion of the NATO Summit in Vilnius. According to the experts, this could be due to Russia's failures in the war against Ukraine, which has shifted its focus towards maintaining the attention and support of the Russian public, as well as the upcoming elections in Russia.

The main topics that dominated 2023 were the following: the war in Ukraine (a general topic that includes many subtopics, such as Western as well as Lithuanian military aid to Ukraine, disinformation that NATO troops are fighting in Ukraine, or fake news about the destruction of NATO centres, deaths of NATO troops, alleged reluctance to help Ukraine, etc.); NATO, as well as NATO-Russia relations and the NATO Summit in Vilnius; Lithuania's NATO membership; Lithuania-Belarus relations; and Lithuania-Russia relations, State governance and order. These topics have been developed in previous years.

The general trend in 2023 shows that Russia's attention to Lithuania's information space is declining, but it is too early to say whether this is only a temporary 'retreat'. According to the experts, the Lithuanian society is well aware and understands that Russia is fighting a brutal war not only in Ukraine but also in an aggressive information war against us and Western civilisation. Yet, it is unable to overcome the fear of Russia. Russia is spreading this fear through propaganda channels and disinformation methods, with its dominant messages being that war with the West is inevitable, that the Baltic States will be attacked first, and that NATO (the West) will provoke Russia into a nuclear strike and World War III. According to the experts, the **average score of Russia's influence on Lithuania's information environment was 3.5 points.**

## Number of Russian-Controlled Information Channels and their Audience in Lithuania

Among the sanctions imposed on Russia in 2022 was a ban on Russian propaganda TV channels: The EU Council imposed sanctions on the following Russian TV channels: RT (Russia Today), Sputnik, Rossiya RTR / RTR Planeta, Rossiya 24 / Russia 24, TV Centre International, NTV / NTV Mir, Rossiya 1, REN TV and Pervyi Kanal. The retransmission of programmes on these channels was also banned in Lithuania.

Another step towards an almost total ban on the broadcasting of media controlled by the Russian regime in Lithuania was taken in 2022. On 8 March 2023, the Lithuanian Radio and Television Commission (LRTC) adopted a decision to issue binding instructions to internet service providers to remove the ability to access IP addresses. They imposed administrative and criminal penalties for breaches of the international sanctions. However, in Lithuania, it is possible to watch Russian channels via various websites or on IPTV set-top boxes; the latter are particularly popular among the Russian-speaking audience in Lithuania.

According to the 2022 report of the LRTC, Kantar, a company that conducts research on the audiences of information channels and has conducted public opinion polls, it was found that the viewing habits of those watching TV programmes rebroadcast in the Russian language have changed in Lithuania. Russian-language programmes retransmitted in Lithuania have lost about half of their audience: 50% of the respondents who used to watch them stated that they no longer watch these programmes, as they consider the information they contained unreliable, and noted that they were full of propaganda and misinformation. In addition, 60% of the people who had previously watched such programmes did not miss them. In fact, as late as mid-2022, it was possible to find some Russian TV channels being rebroadcast by regional cable TV stations. Although Russian channels can still be found in some cable and digital packages, their share of the overall supply is very small.

On 9 March 2022, the Lithuanian Radio and Television Commission warned 60 websites to be taken down within five days, due to Russia's aggression in Ukraine and the disinformation and propaganda being disseminated by portals under its control. The Internet Media Association identified sputniknews.lt, sputniknews.ru, ekspertai.eu, lenta.ru, tvzveda.ru and several other websites as unreliable. It was also asked to restrict the information on pages that were registered in Lithuania but often published Russian propaganda (e.g. [laisvaslaikrastis.lt](http://laisvaslaikrastis.lt), [bukimevieningi.lt](http://bukimevieningi.lt), [musutv.lt](http://musutv.lt) (this page has been blocked), [ausra.ifo](http://ausra.ifo), [kazimierasjuraitis.lt](http://kazimierasjuraitis.lt), [nepriklausomizurnalistai.eu](http://nepriklausomizurnalistai.eu), [3min.lt](http://3min.lt) and [20min.lt](http://20min.lt)). The information supplied by some of these pages was available not only in Lithuanian but also in Russian. Most of them are currently inaccessible.

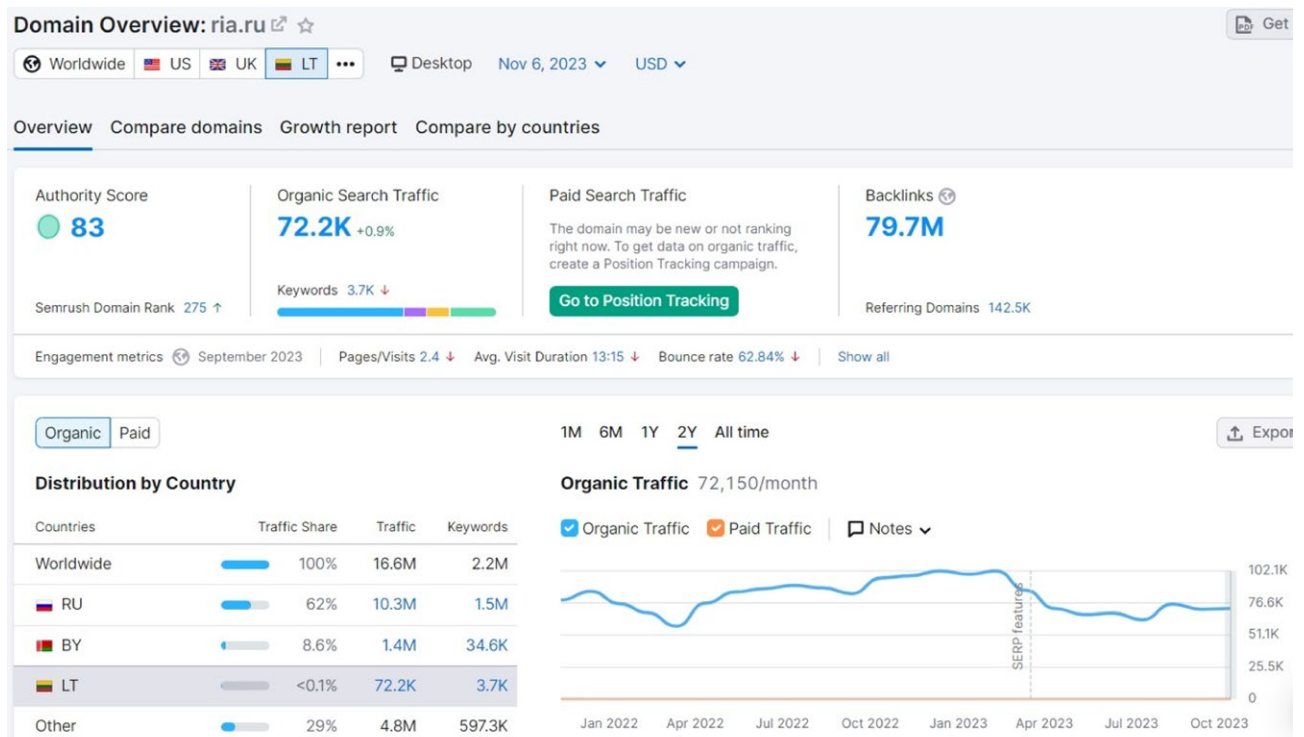
**Table 2.** Audience of Russian TV channels in Lithuania from 2018-2022

Year	TV channels						Share of the TV audience
	PBK	NTV Mir Lietuva	REN Lietuva	TNT	Dom Kino	New Time Media	TNT
2022*	-	-	-	-	-	-	-
2021	6.3	4.6	3.7	2.7	2.4	4.8	0.5
2020	7.3	5.8	4.6	2.8	2.8	5.8	0.6
2019	7.1	6.1	3.8	2.5	2.5	5.5	0.4
2018	7.6	6.0	3.9	0.7	0.4	4.9	0.1

Source: 'Kantar'

\* – due to the sanctions imposed on Russia, Russian channels cannot be broadcast in Lithuania.

**Fig. 5.** User traffic of the Russian news portal ria.ru in Lithuania



Source: <https://www.semrush.com/>

However, some websites still make it possible to read Russian media portals. One of them is rubaltic.ru, a website available not only in Lithuania, but also in other Baltic countries. The three most popular Russian websites in Lithuania are ria.ru, lenta.ru and rbr.ru.

Ria.ru has the largest audience of the three monitored websites in Lithuania, with an average monthly traffic of 72 thousand in 2023. It should be noted that there was a decrease between February and April 2022; however, it has since not only returned to its original level but has increased to 102 thousand users per month (January 2023 data).

Lenta.ru – average traffic in 2022 was 51,297. Following the outbreak of the war, the access to this website increased. This year, the trend has reversed, dropping 10 thousand logins since April and almost 31 thousand users in September.

Rbr.ru – this Russian website is the least visited of the selected ones, with an average monthly traffic of 19.25 thousand in 2022. The figure for this year was around 16 thousand.

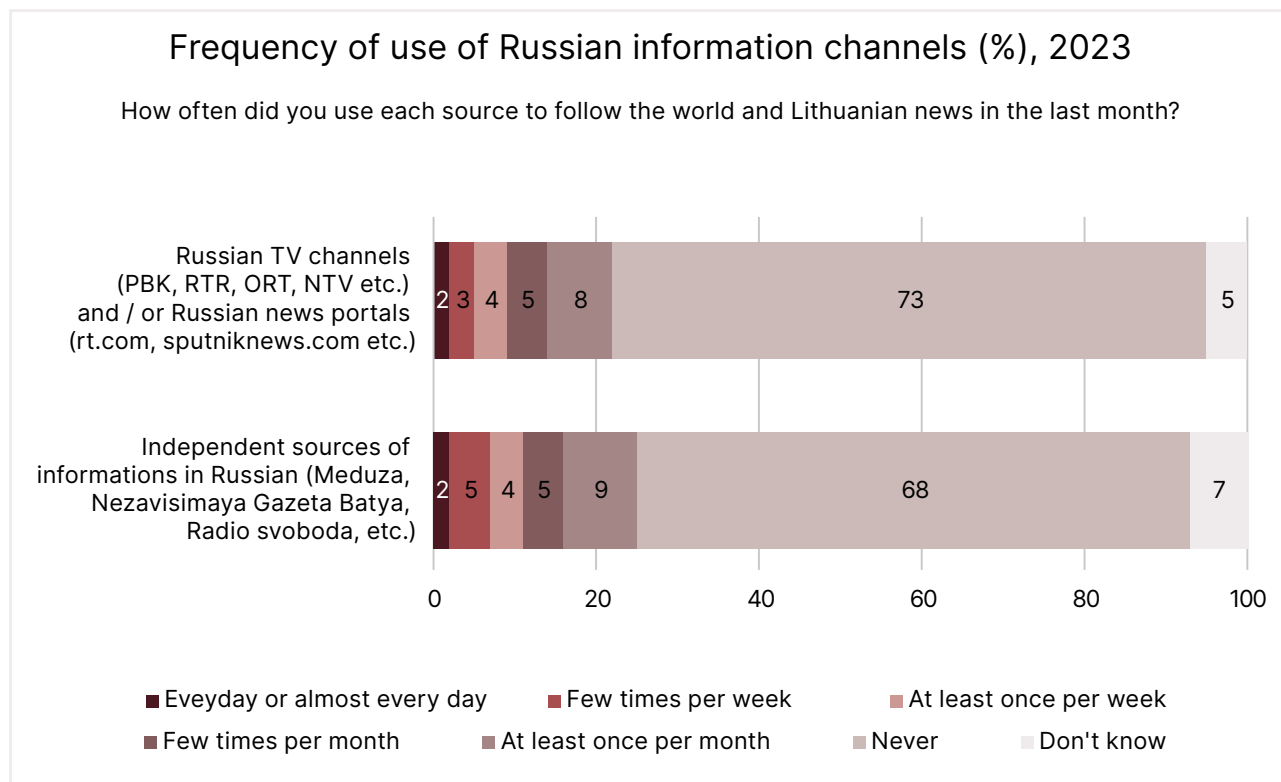
Although Lithuanian online audience companies (e.g. GEMIUS) do not audit Russian websites, the traffic from Lithuania is still significant. Although this is not a large number in terms of the overall internet traffic, the use of Russian media in Lithuania has not completely stopped. It is reasonable to assume that, on average, Russian information portals have a monthly traffic of around 100-200 thousand users from Lithuania.

**After summarising the potential audience for Russian information flows in Lithuania, 2 points were allocated for using online sources and IPTV set-top boxes.**

## Use of Russian Media in the Lithuanian Information Space

In September 2023, Spinter, a public opinion research company commissioned by the Eastern Europe Studies Centre, conducted a survey asking, among other questions, what information sources the Lithuanian population uses. Of course, Lithuanian information channels were the most used media. Still, the Russian media was also being followed. Summarising a number of possible options based on the frequency of using Russian information sources, 22% of the Lithuanian population surveyed follow the official, regime-sponsored TV channels or online news sites at least once a month (or more often) (73% did not follow at all, and 5% could not respond). It is not difficult to see that the Russian respondents were much more likely to use information disseminated by the Russian official channels (at least once a month – 65%) than the Lithuanians (18%) or Poles (25%).

**Fig 6.** Frequency of use of Russian information channels in 2023



Source: Spinter, 2023

It is worth noting that since 2020, when an almost identical survey was carried out, the use of Russian channels (TV and online sources) to follow the world and Lithuanian news has decreased by about one-third. At that time, 36% of the respondents followed Russian TV at least once a month, while 23% followed online news sites. However, despite the radical restrictions on Russian sources as of February 2022, their use in Lithuania remains quite significant.

Interestingly, independent Russian news channels (e.g. Meduza, Nezavisimaya Gazeta, Radio Svoboda, etc.) are also used by a significant share of the Lithuanian population (25% visit them at least once a month). However, this share has shrunk since 2020, as a few years ago, the share of users of such media was 29%.

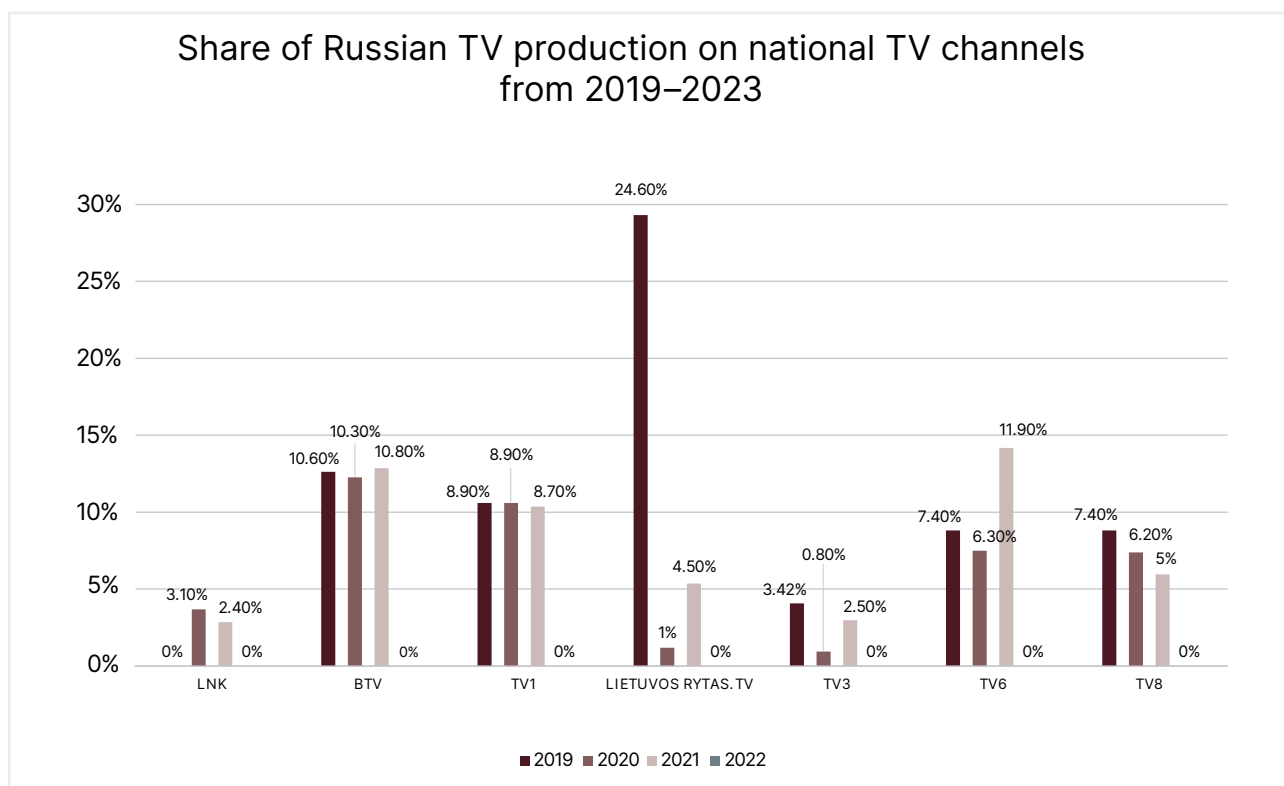
Considering the data from the surveys mentioned above (official Russian media consumption habits), **the score in this category was 2.2 out of 10.**

## Share of Russian-Origin Productions on National TV

For quite a long time, Lithuanian television did not avoid including Russian productions in its programmes, including TV series, films, talk shows, etc. For some time, such programmes or films were broadcast in the original (Russian) language, with subtitled translations. Later, there was a switch to audio dubbing. In many cases, representatives of the Lithuanian TV stations argued that Russian-origin productions were attractive both for the audience and because of their competitive prices compared to similar content produced in the West. Some TV stations broadcasted up to a quarter of their total output of Russian origin, particularly in 2019.

The penetration of Russian productions into Lithuania's information space has long been recognised as a potential threat in Lithuania, which is why a decade ago, it was decided to regulate the origin of broadcast products.

**Fig. 7** Share of Russian TV production on national TV channels from 2019-2021



\*TV channels with no Russian productions: LRT TELEVIZIJA, LRT PLIUS, Info TV, Delfi TV and 2TV

Data from LRTC surveys

According to the Law on Public Information of the Republic of Lithuania, in 2006, it was decided that television broadcasters should devote more than half of the programme time, minus the time for news, sports, games, advertising, teletext services and teleshopping, to European productions, whenever possible. However, it has been noted that TV broadcasters are not strictly obliged to comply with these provisions. In 2017, a group of members of the Seimas registered an amendment to the law to make it compulsory for more than half of the TV airtime to be of European origin. According to them, a survey conducted by the Lithuanian Radio and Television Commission (LRTC) in March 2017 showed that two national TV channels devote more than a third (35.5-38%) of their total weekly TV programme time and about half (44-49%) of their daily time to Russian productions.

Since then, the situation in Lithuanian television has changed significantly. As part of monitoring the share of European productions shown on national television programmes, the LRTC also checks the share of Russian productions. By 2022, the share of Russian-origin productions on Lithuanian TV had dropped to 0%. According to the representatives of the LRTC, although the investigation on 2023 has not yet been finalised, it can be stated that all 12 national television programmes (LRT TELEVISION, LRT PLUS, Info TV, Delfi TV, 2TV, LNK, BTV, TV1, TV3, TV6, TV8 and Lietuvos rytas.tv) did not broadcast any Russian productions. Accordingly, **the score for this indicator is 1.**

Index of the influence on the information domain	2.2 out of 10
Russian information campaigns against Lithuania ( <i>average of the expert assessments</i> )	3.5
Number of Russian-controlled information channels and their audience in Lithuania	2
Use of Russian media in the Lithuanian information space	2.2
Share of Russian-origin productions on national TV	1

## Societal Security

Index of the influence on societal security

3.6 out of 10

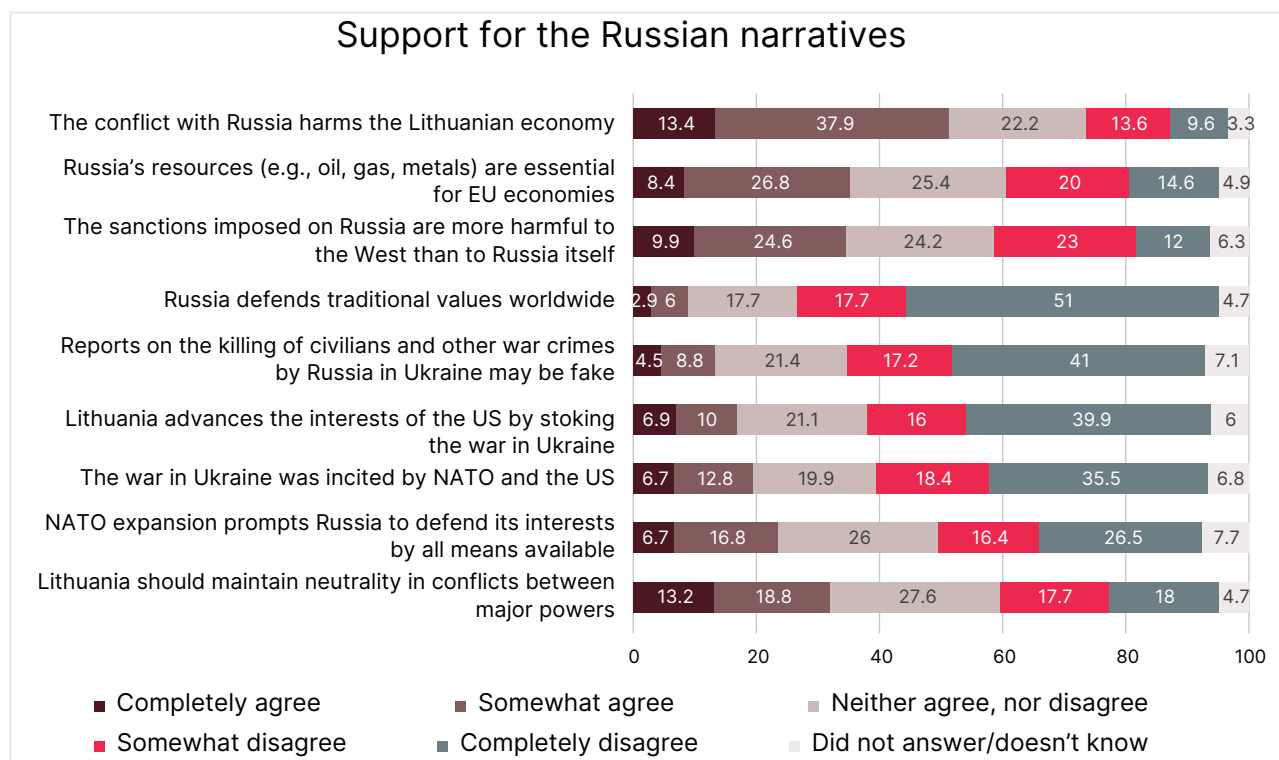
Societal security can be defined as the preservation of a society's identity and functionality. Russia's influence on the functionality and identity of Lithuania's society can be assessed in terms of the factors that trigger destructive processes aimed at denying democratic values and dividing society.

### Public Support for the Russian Narrative

In September 2023, Spinter, a public opinion research company commissioned by the East European Studies Centre, carried out a poll in which part of the questions were aimed at finding out to what extent typical Russian narratives – statements against Lithuania, Western countries and Euro-Atlantic alliances, aimed at raising public discontent with the Lithuanian government, Euro-Atlantic orientation and democratic values – are supported by the Lithuanian society.

Among the typical Russian propaganda narratives, the most frequently supported were statements related to subjective assessments of the economic damage allegedly suffered by Lithuania or Western countries, as a result of the conflict with Russia. For example, more than 51% of the respondents agreed or strongly agreed with the statement that 'Conflict with Russia hurts Lithuania's economy', 35% agreed or strongly agreed with the statement that 'Russia's resources (e.g. oil, gas, metals) are essential for the EU economies', and 34.5% agreed or strongly agreed with the statement that 'Russia's sanctions are more harmful to the West than to Russia itself'. The statements that 'Russia defends traditional values in the world' (8.9%) and Russia's favourite narrative that 'Reports of civilian killings and other Russian war crimes in Ukraine may have been fabricated' received the least support.

**Fig. 8** Support for the Russian narratives in Lithuania in 2023



Source: EESC/Spinter survey, September 2023

The overall average agreement (i.e. the average sum of those who agreed or strongly agreed with the statements) for all statements included in the survey was 26.1%. Accordingly, **the score of support for the Russian narrative in Lithuanian society is 2.6.**

### Level of Acceptance of Democratic Values

The strength of a democratic society comes from its support for fundamental democratic principles. It is these principles that Russia's authoritarian regimes often target in their attempts to destabilise societies abroad. The greater the public acceptance of democratic values, the harder it is for Russia (or other authoritarian countries) to spread its ideology, divide the public, and achieve general social and political damage.

**Table 3.** Necessity of democratic features survey, 2023

Element	Average	% of the respondents selected an 'essential characteristic of democracy.'
<i>Liberal democracy</i>		
Citizens have the right to freely and openly express opinions and beliefs, including criticism of the government	8.7	58.6
People elect their representatives in free elections	8.8	59.8
Women have the same rights as men	8.6	55.6
Courts act impartially and are free from political influence	8.5	52.7
The rule of law prevails in the country	8.3	47.5
The rights of ethnic minorities are guaranteed	8.0	38.8
Two or more political parties compete in an election	8.3	50



Element	Average	% of the respondents selected an 'essential characteristic of democracy.'
<i>Accountability of the democratic government</i>		
When making decisions, the government takes the views of the population into account	8.4	46.9
Citizens can get involved in and influence the government's decision-making	8.2	43.9
The government justifies its policies to the public	8.4	47.9

Source: EESC survey 'Democracy Barometer', 2023.

The East European Studies Centre has been conducting the Democracy Barometer survey since 2022 to measure the Lithuanian society's support for democratic values and its resistance to authoritarian narratives. Part of this survey focuses on the perceptions of liberal democratic principles (the Liberal Democracy Perceptions Index), which is used as an indicator for this category. The Democracy Perceptions Index asks the respondents to rate the necessity of various elements of the institutions of liberal democracy (political and civil rights), representation and accountability, social justice and direct democracy on a scale from 1 to 10.

Political and civil rights – such as the freedom of opinion and expression, free elections, and women's and men's rights – are seen by Lithuanians as the most essential features of democracy. Their average score was between 8.6 and 8.8, and between 55% and 59% of the respondents chose these elements as essential features. The assessment of the impartiality of the judiciary was not far behind (average 8.5). Among the institutions of liberal democracy, the rights of national minorities were perceived as the least necessary (38.8%), but the average for this aspect was still quite high (8).

The final value of the 2023 Liberal Democracy Perception Index was 82.5 (out of a maximum of 100). Since the Russian influence on Lithuania index requires espousing opposite values, after inverting the Liberal Democracy Index and converting it into a ten-point system  $((100-82.5)/10)$ , **the score is 1.75**.

## Civic Empowerment Index

The Civic Empowerment Index (CEI) is a model developed in Lithuania by experts at the Civil Society Institute, including Dr Mindaugas Degutis, Dr Aina Ramonaitė and Dr Rūta Žiliukaitė. It measures the civic and social engagement of the Lithuanian population. In 2022, the study showed a slight decrease in the total CEI despite Lithuania's active involvement in delivering assistance to Ukraine. The index reflects a range of societal factors that influence civic engagement. Although Lithuania has consistently engaged in civic activities, the decline in the CEI may be a sign of the public's frustration with the overall effectiveness of the democratic system, which is reflected in a decline in active participation and engagement in political and social activities.

The indicator measuring the public's real and potential engagement, sense of their own influence, and their assessment of the risks associated with civic engagement scored 35.9 out of a possible 100 in 2022. This is the lowest value since 2017 when the index stood at 37 points. In 2021, the index reached a record high of 41.3 points (the 2023 results have not yet been published).

By applying the inversion of the Civic Democracy Index and converting it into a ten-point system, **the average score is 6.4**, reflecting the 'passivity' of the Lithuanian society, which may be weaponised by Russia in spreading its influence.

Index of the impact on societal security	3.6 out of 10
Public support for the Russian narrative	<b>2.6</b>
Level of acceptance of democratic values (inverted value)	<b>1.75</b>
Civic empowerment index (inverted value)	<b>6.4</b>

## Political Domain

Index of the influence  
on the political domain

**3.4 out of 10**

The concept of political security and, consequently, the assessment of external influences on the political domain of the functioning of the state is highly ambiguous. It depends on deciding what we consider to be the essential (protectable) objects of the political system – safeguarding democracy, political stability, the effectiveness of the political system, or the maintenance of the balance of power. In the classic sense, according to Barry Buzan's definition, political security involves the organisational stability of the state, the effective functioning of government systems and the establishment of ideologies that support the government's legitimacy. In this study, the impact on the Lithuanian political domain, despite the complexity of this concept, has been summarised according to 5 indicators, which may reflect the direct interference in the process of representative/procedural democracy (through attempts to influence the electoral process), and the indirect impact through actors in the political system (parties), as well as the possibility of corrupting the political system or reducing the overall public trust in state institutions (and thus reducing the links between the society and the state).

### Vulnerability of the Electoral System to External Influences

In democratic countries, the results of national elections have perhaps the greatest impact on political attitudes, national programmes and decisions. As the precedents of the last decade show, Russia actively interferes in the elections in various Western countries. Although the results of this Russian influence are not always directly observable and can, at best, be detected after the fact, it is assumed that the resilience of the electoral system to illegal interference in the electoral process is the best indicator of the potential for an external influence.

Back in 2020, the East European Studies Centre carried out a study on '[External Threats and Risk Factors in the Lithuanian Electoral Context](#)', which looked at the most important trends in external interference

during the last decade, the response measures, and the experience and needs of Lithuania in dealing with potential interference in its elections. The study found that, although the Lithuanian electoral process is regulated in perhaps the most stringent way in Europe (with bans on legal persons financing election campaigns; relatively strict ceilings on the permissible expenses of participants in electoral campaigns; the introduction of criminal liability for the unlawful financing of political parties and campaigns as of 1 January 2020; tougher administrative fines and the extension of the possibilities for the Central Electoral Commission (CEC) to reduce or eliminate the state subsidy to political parties in case of breaches of the rules), risks to the electoral process and the results of the elections remain. While it is true that major risks of harm – for example, compromising all election results – were assessed as a low probability in 2020, the potential for interference in the electoral process by increasing the polarisation and tension in society, as well as by contributing to the compromising of individual politicians and parties, and by slandering them in the information space, were identified as highly probable (see the summary of the risk assessment from the 2020 survey).

In the survey and interviews conducted with the experts in the autumn of 2023, the possibilities of influencing or compromising the electoral procedures due to the 'human factor' – for example, by exploiting the members of individual electoral commissions, who could purposely seek to hinder the electoral process or to change the electoral results, or by becoming the target of a cyber-attack on the CEC's electoral results processing systems (the electoral results are entered into, and processed by, a separate information system that is accessed by the members of the electoral commissions at the district and regional levels only) – were the issues mentioned most often. However, risks of a systemic nature and potential external effects were rarely mentioned. As has been argued, foreign funding is limited and controlled to the maximum extent possible, the public is critical and judgmental, there are no significant organisations of influence, and the impact can only be made through individual actors. Previous cases have shown that the CEC has the means to counteract documented undue influence on election results by simply not accepting the results of elections in individual districts or even regions, so the essential safeguards of electoral credibility are working effectively. It was also pointed out that Lithuania does not yet have general online voting, which reduces the potential impact of threats through cy-

ber means. One of the most frequently mentioned means of influence was activity on social networking platforms by spreading disinformation or attempting to discredit some election participants. The subjective assessments provided by the experts on the extent to which Russian entities or Russian-dependent actors can influence the electoral process and/or results at the national level in Lithuania resulted in **an average score of 4.1**.

## Public Mistrust of State Institutions

The legitimacy of state institutions is reflected in the public's trust in those institutions. The lower the public's trust in key government institutions, the greater the risk that the fractured links between the state and society will occur, preventing the political stability necessary for the effective functioning of the state. This classic principle of political security, formulated by Buzan, is also being exploited by Russia in a very targeted way: the aim of all disinformation, propaganda and destructive information campaigns is ultimately to break the links between society and state institutions, to cast doubt on the legitimacy of democracy, and thus potentially even to eliminate the foundations of the statehood.

Of course, trust or mistrust in state institutions is not solely the result of Russian influence. However, this indicator is an important criterion for projecting Russia's 'sharp' power – the higher the level of distrust in state institutions, the greater the potential to trigger and provoke protests or disobedience to official decisions by groups in a society.

Data from a survey conducted by Spinter for the East European Studies Centre (20 September to 9 October 2023) shows that the level of distrust in

the main Lithuanian government institutions is quite high. The Seimas and the government are the most distrusted entities, with 69% and 60%, respectively. In addition, 42% do not trust the courts, and 44% do not trust the institution of the President.

The average level of distrust in state institutions is 54%, leading to a **score of 5.4** for this category.

## Political Attitudes of the Parliamentary Parties

The political attitudes of the main political parties (represented in the Seimas) towards Russia, EU and NATO membership and the upholding of traditional democratic principles reflect the tendency of the political elite to support or oppose the narratives promoted by Russia (and could indirectly reflect Russia's invisible influence on the country's politicians and political parties).

Although Lithuania's national politics are dominated by overtly anti-Russian attitudes, and anti-Russia narratives are more or less common to virtually all the major political parties, some manifestations of implicit support for the Russian narratives can be observed. This does not imply that one or another party has direct links with or is directly influenced by Russian entities. However, some narratives, even those that emerge organically from the internal attitudes, worldviews or ideologies of party members, can be exploited and weaponised by the Russians. It is done by reinforcing them, multiplying them, promoting confrontational positions within society, and so on.

Nonetheless, it should be noted that the assessment of this category is highly subjective, based on the experts' subjective, generalised assessments. To

**Table 4.** Level of trust and distrust in Lithuanian state institutions, %

	Trust very much	Trust	Do not trust	Do not trust at all	Do not know	Do not trust
Institution of the President	4.7	45	32.8	11.5	5.9	44.3
Seimas	1.9	22.7	44.1	25	6.3	69.1
The courts	4.6	45.4	32.3	10	7.7	42.3
The government	3.6	30	38.2	22	6.1	60.2
<b>Average</b>						<b>53.98</b>

Source: Democracy Sustainability Barometer 2023

**Table 5.** Favourability of the parliamentary parties' political attitudes towards Russia's interests

	Average of the expert assessments	Number of representatives in Parliament*	Weighted average
Labour Party	5	8	0.28
Union of Democrats 'For Lithuania'	2.27	17	0.27
Freedom Party	1.64	10	0.12
Liberal Movement	1.45	12	0.12
Electoral Action of Poles in Lithuania – Christian Families Alliance	6.1	3	0.13
Lithuanian Regions Party	4.45	2	0.06
Social Democratic Party of Lithuania	2.27	13	0.21
Lithuanian Farmers and Greens Union	4	19	0.54
Political Party 'Freedom and Justice'	4.55	1	0.03
Homeland Union – Lithuanian Christian Democrats	1.36	50.0	0.48
<b>Aggregate average</b>			<b>2.25</b>

\* As of 28 November 2023

Source: EESC expert survey, November 2023

form this assessment, Lithuanian politicians conducting research in national politics, the party system and parliament were interviewed (in total, more than 20 political scientists and experts were invited to participate in the survey). On a scale of 1 to 10, they were asked to rate the extent to which the political attitudes of parliamentary parties are likely to be favourable to Russian interests.

According to the experts' assessments, the least favourable to Russia's interests are the attitudes of the Homeland Union, with an average score of only 1.36 out of 10 possible points. The experts ranked the Electoral Action of Poles in Lithuania – Christian Families Alliance as the closest party to Russia's interests (with an average score of 6.1).

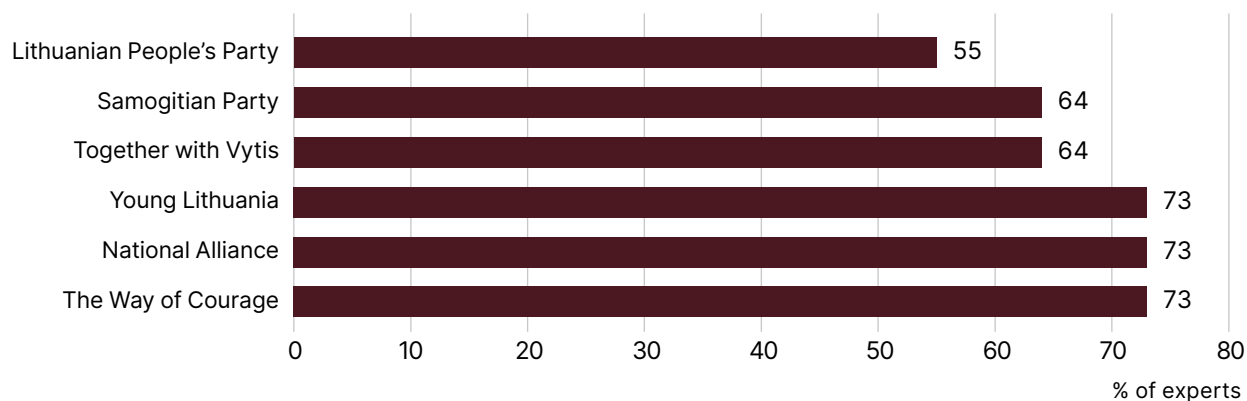
When calculating the final score for this category, it was important to consider the weight of the parties in the Seimas, i.e., the number of seats they hold. Naturally, the more a party is represented in the Seimas, the more influence it has on the final, national-level decisions and policies the Seimas implement. Accordingly, a weighted average of the experts' assessments was calculated as the 'weight' of the provisions concerning the ratio of the number of seats they hold to the sum of the number of members of the Seimas (141). The weighted averages were considered and combined to give an overall average for this category of **2.25 points**.

## Popularity of Radical Parties

As the [research on sharp power](#) shows, radical parties or movements are one of the main platforms for Russian (and also Chinese) manipulation. Radical left- and right-wing parties are actively used in Russia's malicious policies to promote social division, distrust of the EU and NATO, and an opposition to human rights. The level of support for radical and explicitly nationalist parties (public support) directly correlates with the potential Russian influence.

In assessing this category, it has to be stressed that political 'radicalism' is a rather complex phenomenon and that there are various descriptions and [definitions](#). However, this study was not aimed at providing an academically accurate assessment of the level of radicalism of the Lithuanian political parties, as this would require additional, highly complex research. In this case, the generalised assessments of political scientists studying the political and party system were used. These are comprised of subjective assessments that could potentially reflect the dominant narratives in the societal domain. However, there have been no comprehensive assessments of the radicalism of political parties or movements in Lithuania, so we have to rely on expert opinions. The choice of which officially registered political parties can be considered radical is based on an expert

**Fig 9.** In your opinion, which of these officially registered political parties can be considered to be radical parties?



Source: EESC expert survey, November 2023

consensus based on a survey of political scientists (more than 20 political scientists were invited to participate). We followed the principle that if more than 50% of the political analysts surveyed identified a particular party, we would classify it as radical.

According to data from the Ministry of Justice, in November 2023, 27 political parties were officially registered, 23 of them were active, three were in the process of liquidation (the Lithuanian Political Prisoners' Party, People's Unity Party, and the Order and Justice Party), and one (the Russian Alliance) had asked to initiate liquidation. Five officially active parties were identified as radical by more than 50% of the surveyed experts: The Way of Courage; National Union; Young Lithuania party; the political party 'Together with Vytis'; Samogitian Party and the Lithuanian People's Party. Political movements were not included in the survey, as they are not allowed to participate in elections to the Seimas according to Lithuanian law, and their political activism and activities are mostly confined to the geographical bound-

daries of local municipalities. While some may have a significant political impact, the assumption was that political movements seeking influence at the national level need to transform themselves into a political party and seek representation in the Seimas.

The parties identified by the experts as radical do not have significant support in Lithuanian society. None of them are currently represented in the Seimas. In public opinion surveys, they are not among the parties supported by at least 2-3% of the respondents.

According to the last municipal and parliamentary elections, we can see that the support for these parties is very low, with only the 'National Union' party showing actual activity. According to the Ministry of Justice, the Way of Courage party did not provide the necessary data on the number of party members until 1 October 2023. It is likely that the party, which once had a significant group in the Seimas, may eventually disappear completely.

**Table 6.** Results of the parties considered to be radical (according to expert assessments) in the Seimas and local government elections, % of votes received

	Parliamentary elections in 2020	Municipal elections in 2023
The Way of Courage	1.14	did not participate
National Alliance	2.14%	1.12%
Young Lithuania	did not participate	did not participate
Together with Vytis	did not participate	did not participate
Samogitian Party	did not participate	0.06%
Lithuanian People's Party	0.25%	did not participate

Source: Central Electoral Commission, 2023

Taking these results into account, it can be said that the overall support for radical parties and movements in Lithuania is extremely low: none of them has more than 2% of the public's support, and even together, their combined electoral potential is not likely to reach 5% at the current time. Thus, while radical political forces may occasionally attract public attention by escalating one issue or another – notably by joining various protests – their impact on Lithuanian society is minimal. Accordingly, this category scored **1.5 points**.

## Corruption Index

Corruption is one of the political system's fundamental departures from the democratic process. If corrupt practices are widespread in a country, Russia's ability to influence its political decisions increases dramatically. Through corrupt politicians and civil servants, political decisions, and even national security and foreign policy can be influenced in a 'direct way'. Perhaps the most prominent example of this occurring at the international level is the German Chancellor Gerhard Schröder's links and support for Russian interests in Germany. This obvious, but so far formally and legally unappreciated, case of corruption has even given rise to the generic term 'schröderisation' to describe the 'bribery' of politicians (with money, well-paid positions, business deals, etc.)

In Lithuania, political corruption also has many precedents. The MG Baltic case (involving the representatives of several political parties) and the accusations against the former Director of Kaunas City Administration, Vilius Šiliauskas, for allegedly paying the 'biggest bribe' in the history of independent Lithuania, have attracted the most public attention in recent years.

The starting point for this category was Transparency International's annual Corruption Perceptions Index.

The Corruption Perceptions Index (CPI) aggregates data from a variety of sources to measure the level of perceived corruption in the public sector. The CPI is calculated using 13 different data sources from 12 different institutions. A country's CPI score is calculated as the average of all the standardised scores for the country. The CPI scores are standardised on a scale of 0 to 100, with 0 representing the highest perceived level of corruption and 100 being the lowest.

A country's score is the perceived level of corruption in the public sector, ranging from 0 to 100, where 0 means the country is very corrupt and 100 means it is very clean. [Lithuania's ranking in the CPI for 2022](#) was 33, and its overall score was 62 out of 100. Accordingly, the inverse of the indicator  $((100-62)/10)$  gives a score of **3.8 in the corruption category**.

Index of the influence on the political domain	3.4 out of 10
Vulnerability of the electoral system to external influences	4.1
Popularity of radical parties	1.5
Public mistrust of state institutions	5.4
Favourability of the parliamentary parties' political attitudes towards Russia	2.25
Corruption index (inverted value)	3.8

## Conclusion

The average of the possible **influence of Russia on Lithuania** in 2022-2023 in 7 areas of the state's functioning resulted in **an index score of 3.13 on a 10-point scale** (where 1 is no tangible influence and 10 is the maximum possible influence). Since 24 February 2022, many formal decisions have been taken in Lithuania to formally prohibit a direct Russian influence (e.g. banning the broadcasting of Russian news channels in Lithuania, and the implementation of the EU's economic bans on the trade of some goods and services). However, it can be said that remnants of Russia's influence still remain.

**Table 7.** Index of Russia's influence on Lithuania during 2022-2023

Index of Russia's influence on Lithuania	3.13
Military domain	2.4
Economic Domain	2.2
Energy domain	2.6
Cyber Domain	5.5
Information Domain	2.2
Societal Security	3.6
Political Domain	3.4

According to expert surveys, Russia's greatest potential influence lies in the cyber domain. This relatively high level of influence is mainly due to Russia's ability to exploit various software and hardware security vulnerabilities in Lithuania and carry out targeted cyberattacks and other malicious activities against Lithuania's critical IT and communications infrastructure. The experts also pointed out that, on average, more than half of all cyber incidents targeting Lithuania could be attributed to Russian entities.

However, it should be noted that the cyber domain was the most lacking in 'objective' assessment data compared to the other domains, particularly as the individual category assessments in this domain were based on subjective assessments by top-level cybersecurity professionals and representatives of major IT companies. Accordingly, cyber 'threat' arguments dominated the expert commentary and live interviews. It should also be stressed that cybersecurity in this sense is essentially limited to the critical cyber infrastructure, while the vulnerability of business or private users to a possible Russian influence (from data collection to destructive activities) remains very high.

In the future, when assessing the actual dependence of the cyber domain on Russia, it would be useful to collect data on Russian software and hardware by Lithuanian citizens and businesses. For the time being, such data is not available.

Slightly higher than the final average value of the index was recorded in the domains of both societal security (3.6 out of 10 possible points) and politics (3.4 points).

In the domain of societal security, Russia has the potential to have a substantial impact on Lithuania, due to the relatively passive political-social nature of Lithuanian society (as is reflected in the Civic Empowerment Index and other indicators collected through public opinion polls). On the other hand, it can be documented that Lithuanian society in general does not support or is hostile to the typical Russian propaganda narratives and demonstrates a strong understanding of and support for the principles necessary for democracy. In other words, Lithuanian society has learned to identify Russia as a hostile state, does not succumb to its 'soft' influence and is confidently supportive of democratic principles.

In the political area, the main negative impact is due to the high level of distrust among the Lithuanian society towards key government institutions. This is perhaps the most vulnerable point in political terms – the prevailing distrust of the population towards the authorities could undermine the overall strength of the society's relationship with the state. Furthermore, this is precisely the destructive effect that Russia seeks to have by weakening the links between society and the state through the use of 'sharp' power, by seeking out the sources of public discontent, amplifying them, and increasing the prevalence of confrontation and division within the state. On the other hand, the position of the Lithuanian parliamentary parties is almost completely unfavourable to Russian political interests, and the popularity of radical parties in the national political system is minimal. However, this is subject to change – the elections in Lithuania in 2024 may reveal whether public support for radical attitudes is increasing.

The military, economic and information domains also scored lower than the overall index average. It can be argued that these domains are more immune to Russia's influence, which is mainly due to the restrictions or policy decisions introduced after February 2022, ranging from the almost complete refusal to import Russian energy sources to the sharp drop in the turnover of goods and services, to legal decisions to ban the availability of Russian information sources in Lithuania. The resilience of these areas of state functioning to Russian influence is very high and could even serve as a model for other EU and NATO countries seeking to reduce Russia's influence in their countries.



**Eastern Europe  
Studies Centre**

Established in 2006

ISBN 978-609-96440-3-5



9 786099 644035