



DEFENCE
INTELLIGENCE AND
SECURITY SERVICE
UNDER THE MINISTRY
OF NATIONAL DEFENCE



STATE SECURITY
DEPARTMENT OF
THE REPUBLIC OF
LITHUANIA



2026

NATIONAL THREAT ASSESSMENT



DEFENCE
INTELLIGENCE AND
SECURITY SERVICE
UNDER THE MINISTRY
OF NATIONAL DEFENCE



STATE SECURITY
DEPARTMENT OF
THE REPUBLIC OF
LITHUANIA

2026

NATIONAL THREAT ASSESSMENT

CONTENTS

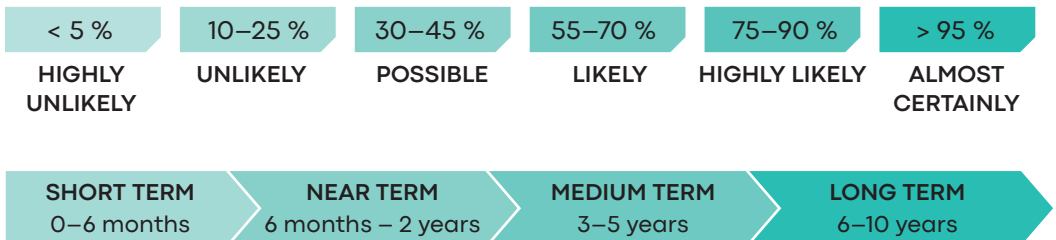
INTRODUCTION	3
FOREWORD	5
SUMMARY	10
RUSSIA	14
BELARUS	38
CHINA	45
ECONOMIC AND ENERGY SECURITY	57
CYBER SECURITY	67
INFLUENCE ACTIVITIES AGAINST LITHUANIA	72
EXTREMISM AND TERRORISM	80

INTRODUCTION

The National Threat Assessment by the Defence Intelligence and Security Service under the Ministry of National Defence of the Republic of Lithuania (AOTD) and the State Security Department of the Republic of Lithuania (VSD) is presented to the public in accordance with Articles 8 and 26 of the Law on Intelligence of the Republic of Lithuania. The document provides con-

solidated, unclassified assessment of threats and risks to national security of the Republic of Lithuania prepared by both intelligence services. The document assesses events, processes, and trends that correspond to the intelligence requirements approved by the State Defence Council. The assessment is based on the information available before February 6, 2026.

THE TABLE BELOW OUTLINES THE LANGUAGE OF PROBABILITY AND DEFINITION OF TERMS USED IN THIS ASSESSMENT:





Colonel Mindaugas MAŽONAS
Director of the Defence Intelligence and
Security Service under the Ministry of National
Defence of Lithuania



Remigijus BRIDIKIS
Director of the State Security Department
of the Republic of Lithuania

FOREWORD

We are facing different kinds of threats ranging from the airspace violation by Russian drones and information operations to cyberattacks and the activities of hostile intelligence services. Still, the security of Lithuania highly depends on the actions of our neighbours, and the most important factor is Russia's long-term determination to increase and, if necessary, use its military power.

Most of Russia's military capabilities are currently concentrated on the front line in Ukraine. However, Russia is still able to continue implementing its Armed Forces reform and increasing its military capabilities in the Kaliningrad Region and near NATO's eastern borders.

The Kremlin would like to expand the Russian Armed Forces as fast as possible, but it has to deal with the consequences of the large-scale war against Ukraine, the struggling economy, and the international sanctions. However, the Russian government is determined to pursue its military goals even at the expense of its citizens' welfare. Increasing taxes and uncontrolled inflation will affect a larger part of the Russian population, who will have to bear the burden of unprecedented military spending.

The conventional military threat to Lithuania is expected to remain low in the near term. However, we must be prepared to address other security challenges. Neighbouring regimes hostile to Lithuania are using unconventional means to influence the minds of our citizens, to create a sense of insecurity, and force us to make decisions that benefit these regimes. The Belarusian regime exploits cigarette smuggling via high-altitude balloons and politically motivated detention of Lithuanian citizens as a means of pressure and intimidation to seek international recognition and reduce restrictions imposed on Belarus.

Moreover, hostile intelligence services continue their operations directed against Lithuania. As their actions on our territory are restricted, hostile intelligence services are trying to recruit our citizens who travel abroad. Anyone, even those without access to classified information, can become their target, so Lithuanian intelligence agencies, like other state institutions, urge citizens to remain vigilant and refrain from travelling to Russia and Belarus.

New technologies that fall into the hands of hostile actors can also pose a threat to our national security. We observe a novel trend of using artificial intelligence tools to carry out complex cyberattacks against crucial Lithuanian institutions.

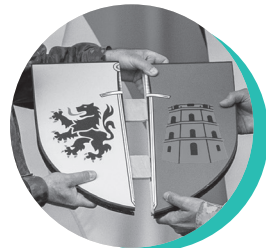
Hostile states are also conducting information operations against Lithuania. Using false narratives and threatening messages, they attempt to spread panic and distrust of state institutions. However, we can thwart the efforts of hostile actors and increase the resilience of society by practising critical thinking, distinguishing facts from false information, and taking an active interest in security issues.

Russia will use the old 'divide and rule' method to pursue its imperial ambitions, for instance, by seeking to disrupt the unity of NATO. The antidote to this is consistent dialogue and closer cooperation, which underlines the shared values of the members of the Alliance.

To deter Russia from reckless military aggression against us or other NATO states, we need to continue to develop our defence capabilities and keep strong ties with NATO partners. Every citizen of Lithuania contributes to increasing our defence potential by developing their ability to identify threats and prevent them. We hope that the information prepared by Lithuania's intelligence community and presented in this assessment will be relevant and useful.

Key events related to the security of the region

JANUARY	FEBRUARY	MARCH	APRIL	MAY	JUNE
<p>26th After unrecognised presidential election, Alexander Lukashenka remains in power</p>	<p>8th Lithuania and the Baltic States disconnected from BRELL energy system</p>	<p>2nd European countries established the Coalition of the Willing to provide support and security guarantees to Ukraine</p>	<p>10th GRU illegal Eduard Manov was convicted of spying for Russia and sentenced to imprisonment</p>	<p>13rd A Russian fighter jet violated NATO airspace during the incident with a shadow fleet vessel in Estonian territorial waters</p> <p>14th The EU adopted the 17th package of sanctions against Russia</p>	<p>1st Ukraine launched operation 'Spiderweb' (a massive drone attack on Russian military airfields)</p> <p>2nd The second negotiation meeting between Ukrainian and Russian delegations took place</p>
<p>27th The Latvian fibre-optic cable connecting Latvia and Sweden was damaged</p>		<p>5th French President Emmanuel Macron proposed the idea of a European nuclear umbrella</p> <p>13th A meeting between Putin and Lukashenka took place in Moscow – the security guarantee agreement signed by both sides in December 2024 came into force</p> <p>24th The EU ban on the transit of Russian liquefied natural gas through its ports to other countries came into force</p>	<p>26th Russia acknowledged the participation of North Korean soldiers in military operations against Ukrainian forces in the Kursk Region</p>	<p>15th The first negotiation meeting between Ukrainian and Russian delegations took place</p> <p>22nd The Official inauguration of Germany's 45th Armoured Brigade 'Lithuania' was held</p>	<p>15th A Russian warship for the first time openly escorted shadow fleet tankers in European waters</p> <p>21st US Special Envoy for Ukraine Keith Kellogg visited Belarus</p> <p>24th and 25th At the Hague summit, NATO allies committed to allocating 5 percent of GDP to defence and related infrastructure funding</p>





10th

A Russian Gerbera drone crashed in Lithuanian territory

18th

The EU adopted the 18th package of sanctions against Russia

4th

Russia announced that it would no longer adhere to its unilateral moratorium on the deployment of intermediate-range nuclear missiles

9-10th

Russian UAV violated Polish airspace, prompting NATO consultations

11th

NATO launched a new airspace defence mission Eastern Sentry in Eastern Europe

22nd

Russia held its annual nuclear triad exercises

23rd

Russian Il-78 aircraft violated Lithuanian airspace

24th

The Ukrainian citizen Daniil Bardadim was convicted of arson at the IKEA store in Vilnius, and the aim of carrying out terrorist acts in Lithuania and Latvia

18th

Belarus announced the deployment of the Oreshnik missile system on its territory

JULY

AUGUST

SEPTEMBER

OCTOBER

NOVEMBER

DECEMBER

23rd-27th

The Russian Navy conducted operational exercise 'July Storm'

28th

The second Gerbera drone carrying an explosive charge crashed in Lithuanian territory

12-16th

The active phase of the strategic Russian-Belarusian exercise 'Zapad 2025' took place

19th

Three Russian MIG-31 fighter jets violated Estonian airspace, prompting NATO consultations

23rd

Russia proposed a one-year extension of the New START nuclear arms control treaty

23rd

The EU adopted the 19th package of sanctions against Russia

26th and 29th

Russia conducted tests of the Burevestnik and Poseidon nuclear delivery vehicles

27th

Lithuania officially withdrew from the Ottawa Convention, which prohibits the use, stockpiling, and production of anti-personnel mines



SUMMARY

■ **Russia's military build-up is the most significant factor determining the security situation in Lithuania and the region.** Currently, the growth of Russia's military capabilities is restricted, as almost all of Russia's available resources are allocated for the war efforts; therefore, its ability to pose military threats to other countries remains temporarily limited. However, this may change depending on the situation at the front.

■ **Currently, Russia's military industry is capable of supplying the army in the field and supporting the development of the Armed Forces.** It remains dependent on foreign technology, materials, and components, and some of these dependencies are expected to remain in the long term. However, the Kremlin is increasing its resistance to sanctions by investing in technological independence.

■ **Although the Belarusian regime has expressed an interest in improving relations with Western countries, it almost certainly does not intend to soften its authoritarian policies.** The regime's attempts to normalise relations with the West are motivated by political and economic interests. Proving the legitimacy of his rule and easing the sanctions on Belarus are essential to Lukashenka. Despite the interest in improving relations with the West, Belarus's policies and actions towards Lithuania and neighbouring countries are highly likely to remain aggressive in the near term.

■ **The Belarusian regime compiles extremist watchlists to suppress the democratic opposition.** These lists include not only Belarusians who on political grounds have been convicted of criticising the regime or having links to the democratic opposition but also individuals and entities from other countries. Anyone who is on the lists or has connections with those included faces the threat of arrest in Belarus.

■ **By increasing its military and geopolitical influence, China seeks to create an alternative world order.** To achieve this goal, Beijing is making efforts to take over the leadership of a bloc of countries that are hostile to the West. China is expanding its cooperation with Russia in order to gain greater influence in the Indian and Pacific regions and globally. Intelligence activities, data collection and information censorship pose security risks to Lithuanian citizens both in China and in Lithuania. It is highly likely that Beijing's influence will grow in the near term; and attempts to form an alternative world system will become more pronounced, which will increase geopolitical tensions.

■ **Entities working against Lithuania's national security interests continue to look for new opportunities to gain access to sectors or infrastructure of strategic importance.** One of the methods involves establishing business contacts with entrepreneurs from other European countries or the US, then using them as intermediaries to avoid direct participation and creating a positive image of a business initiative. Russian and Belarusian entities are also seeking to use companies established in Lithuania for acquiring and further developing Western technologies. Their interest in obtaining Western technologies will remain particularly high.

- **Coordinated cyber espionage groups from hostile states pose a threat by attempting to steal information from Lithuanian organisations, to spread disinformation, and prepare for destructive operations.** The damage caused by cyberattacks is exacerbated by the vulnerability of supply chains and growing use of new technologies such as artificial intelligence. It is almost certain that with increasing effectiveness of cyber capabilities, organisations unable to adapt to a rapidly changing environment will most significantly face cyber threats.

- **Russia has repeatedly accused the Baltic States of systematically distorting the history of World War II, glorifying Nazi collaborators, and persecuting Russian speakers.** The Russian Ministry of Foreign Affairs plays a key role in disseminating these accusations within international institutions. Through public statements and diplomatic channels, the ministry seeks to highlight the alleged Russophobic policies of the Baltic States. Russia is exploiting these accusations in an attempt to exert pressure on Lithuania and other Baltic States and is likely seeking to justify its aggressive foreign policy and geopolitical interests.

- **Islamist terrorist organisations and right-wing extremists are increasingly seeking to recruit minors.** In recent years, several attempts have been identified in Lithuania to establish groups promoting nihilistic right-wing extremism, whose followers are often very young individuals. The spread of right-wing extremist ideology is increasing the likelihood of 'lone wolf' attacks. Islamist terrorist organisations and their supporters use new technologies, such as artificial intelligence, to create violent content that appeals to minors. In the near term, terrorist propaganda disseminated via social networks and gaming platforms almost certainly will encourage minors to become involved in terrorist activities.



Photo by the Ministry of National Defence of Lithuania



RUSSIA

- **Russia is increasing its military capabilities near NATO's eastern borders and continues to implement the Armed Forces reforms, which includes plans to expand brigades into divisions and form entirely new military units.**
- **Russia's economic growth is slowing down, forcing the country to adjust its current economic model, but it is not abandoning its military ambitions.** With the main contributor to the federal budget – oil and gas sector revenues – declining, Russia is trying to stabilise its public finances by increasing taxes on businesses and residents.
- **The increased use of uncrewed aerial vehicles (UAVs) poses a threat to NATO countries.** Russia's intensified production and use of UAVs in the war against Ukraine has led to an increase in violations of the airspace of Lithuania and other NATO countries. Some UAVs entering Ukrainian territory deviate from their original flight path due to technical malfunctions or effects of electronic warfare (EW) measures and fly into the territory of other countries.
- **Due to the ongoing war in Ukraine, the Russian Federal Security Service has prioritised the collection of military and Ukraine-related intelligence.** By exploiting individuals travelling from Lithuania to Russia, the service collects information on the movement of Lithuanian and NATO Allies' forces, military equipment and personnel in Lithuania, foreign troops and military exercises.
- **Russia is seeking to protect its shadow fleet by warships escorting its tankers and displaying force in response to any attempts by Western authorities to inspect them.** Due to these actions, the situation in the Baltic Sea will highly likely remain tense.

Reduced Western pressure on Moscow would accelerate Russia's preparations for conflict with NATO

The security situation in Lithuania and the region is directly dependent on the course of Russia's war against Ukraine, as it determines Russia's ability to increase its military capabilities. As long as Russia has to allocate most of its available resources to the war, its ability to pose military threats to other countries is limited. However, this may change depending on how Russia's war will evolve.

If Russia continues its military actions against Ukraine with the same intensity as in the last four years, the war will require significant human and financial resources, and Russia's ability to pose military threats to other countries will remain limited. Even while at war, Russia is rebuilding its army and creating new military units, most of which are being sent to fight against Ukraine. In the medium term, Russia is likely to be able to assemble new military units. If the war continues in the long term,

Russia will likely be able to fill the newly created military units with troops and equipment, but strategic reserves of weapons and ammunition needed for a large-scale military conflict with NATO will not be fully restored.

In case of a ceasefire or a frozen conflict, Russia would be able to develop its military capabilities and replenish its ammunition reserves more quickly. In the near term, the number of troops and equipment at permanent military bases, including units near the Baltic States, would increase. In the medium term, new units would be fully staffed and equipped, with priority given to quantity over quality. The strategic weapons and ammunition reserves depleted during the war would be gradually replenished. In the long term, Russia's Armed Forces would not only expand in terms of quantity but also modernise. Most of the strategic weapons and ammunition reserves would be

The build-up of new units in the Russian Armed Forces



SCENARIOS OF THE WAR AGAINST UKRAINE

	Near term 1-2 years	Medium term 3-5 years	Long term 6-10 years
ONGOING WAR			
CEASEFIRE OR FROZEN CONFLICT			
PEACE DEAL AND LIFTED SANCTIONS	 <p>Russian Armed Forces are ready for a limited military action in the Baltic Sea region.</p>		 <p>Russian Armed Forces are ready for a full-scale war against NATO.</p>

Elements of Russian military capabilities



restored. Russia would be able, in this scenario, to build sufficient capabilities to launch a military action against the Baltic States and gain regional superiority at least in the initial stages of the war even without fully implementing its military reform goals. This could encourage the Kremlin to use military force based on the miscalculation and belief that NATO should be unable to respond in time, and the conflict could be localised and quickly ended in Russia's favour, with nuclear deterrence serving as a safeguard.

If the parties sign a peace agreement and international sanctions are lifted, Russia could develop its military capabilities even faster. It could withdraw a

large part of its forces from Ukraine, have greater freedom to dispose of larger financial resources and more easily obtain the technology needed for its war industry. In the near term, newly created military units, including those located near the Baltic States, would be almost fully staffed and equipped. In the medium term, strategic reserves would be rapidly restored and the military industry modernised, with an increasing focus on quality. In the long term, Russia likely would create not only a 30-50 percent larger army than it had before the war but also a relatively modern one. Strategic reserves of weapons and ammunition would be fully restored. Russia would be ready for a conventional military conflict with NATO.

Russia is expanding its military capabilities near NATO's eastern borders despite losses in the war











Despite Russia's significant involvement in the hostilities against Ukraine, the military build-up plans announced in December 2022 are gradually being implemented. According to these plans, brigades along the eastern borders of NATO countries are being expanded into divisions and completely new military units are being formed. The Western Military District is divided into the Leningrad and Moscow Military Districts (MD). In the Leningrad MD, the 44th Army Corps has been formed, which includes a motorised rifle division under its command. A motorised rifle brigade which was part of the 14th Army Corps has been expanded into a division. Two motorized rifle brigades which were part of the 6th Combined Arms Army have been expanded into divisions. The formation of a new missile brigade armed with Iskander-M missile complexes has also begun in the territory of the Leningrad MD. Similar processes are taking place in the Moscow MD, where a new artillery division has been formed.

The expansion of the Armed Forces in Russia also includes the Kaliningrad Region, which is part of the Leningrad

MD. The naval infantry brigade stationed in Kaliningrad is being expanded into a naval infantry division. In the future, the formation of additional units is also planned, which will increase the number of troops and combat equipment deployed in the region. Currently, the Russian military grouping deployed in the Kaliningrad Region remains temporarily weakened. Most of the land component troops and combat equipment have been deployed to fight against Ukraine. The land component units in the Kaliningrad Region are mainly staffed by conscripts and a small number of professional soldiers.

The Kaliningrad Region is also undergoing military infrastructure development, reflecting Russia's long-term plans in the Baltic Sea region. For several years now, the construction of the over-the-horizon radar station 29B6 'Container' has been ongoing, elements of which are being built in several locations in the region. This facility is designed to detect aircraft and missiles in airspace several thousand kilometres away. Once completed, it will increase Russia's capabilities to monitor airspace at long range. In addition to

Expansion of Russian military capabilities along NATO's Eastern Flank in 2022-2025

-  Motorised Rifle Division
-  Newly formed Motorised Rifle Division
-  Tank Division
-  Newly formed Naval infantry Division
-  Missile Brigade
-  Newly formed Missile Brigade
-  Newly formed Artillery Division
-  CAA – Combined Arms Army
-  TA – Tank Army
-  AC – Army Corps

SWEDEN

FINLAND

ESTONIA

LATVIA

LITHUANIA

BELARUS

POLAND

UKRAINE

14 AC

44 AC

6 CAA

Saint Petersburg

MOSCOW
MILITARY
DISTRICT

1 TA

Moscow

20 CAA

LENINGRAD
MILITARY
DISTRICT

11 AC

this facility, other significant facilities are located on the exclave territory: the Voronezh-DM early warning radar, a new type of arsenal with reinforced concrete storage facilities, a logistics base belonging to Russia's strategic reserve, and others.

Most of the newly formed units of the Russian Armed Forces are not fully staffed and are being developed in parts due to a lack of military personnel, combat equipment, and infrastruc-

ture. The newly formed units and the combat equipment allocated to them do not remain at their home garrisons but are sent to participate in combat operations against Ukraine. Despite heavy losses, the expansion of capabilities allows the continuation of combat operations against Ukraine and demonstrates Russia's intention to build capabilities that would allow it to wage a large-scale conventional war against NATO.

Russia actively uses electronic warfare capabilities in Kaliningrad



Since the beginning of Russia's war against Ukraine, Russia's actions have led to an increase in jamming and spoofing of satellite communication. Satellite communication jamming has a negative impact on navigation systems in the Baltic Sea region and Lithuanian territory and may disrupt satellite navigation of military and civilian aircraft, ships, and various other equipment.



In the Kaliningrad Region, Russia actively uses electronic warfare (EW) equipment to jam and spoof satellite

signals at various distances, durations and intensities. The main purpose of using this equipment is to prevent UAV attacks on Russian military facilities and critical civilian infrastructure in the Kaliningrad Region and at sea. Some of these military and civilian facilities are located close to the borders of Lithuania. Russia is aware that its actions have a spillover effect outside the Kaliningrad Region and increase risks to civilian aircraft and shipping in the region. Russia disregards the damage caused by EW equipment and continues to use it.

Development of military infrastructure in the Kaliningrad Region



-  Over-the-horizon radar station
-  Missile defence radar

-  New type arsenal
-  Modern logistics base

War, sanctions, and financial resources limit the development of Russian military industry



The development of Russia's military industry is also being directly hampered by the actions of Ukraine's Armed Forces. In 2025, Ukraine launched intensive attacks not only on Russia's oil refining and logistics infrastructure but also on nearly 50 military industry facilities, some of which were targeted several times. Most of Ukraine's attacks were directed against the production of UAV components and various explosives.

Russian military industry prepares for a new phase of expansion

Since the start of the war, the Russian leadership has mobilised significant administrative and financial resources to expand the production of weapons and equipment needed for the war. As a result, the military industry currently meets at least the minimum requirements in all areas of armaments. Meanwhile, modernisation continues and new production capacities are being built in various sectors (in 2025, military industry companies mainly hired engineers to commission new equipment). The results of these investments will be visible after more time and will have long-term consequences. After the war, Russia's military-industrial complex will move on to the next stage of development, with the state continuing to support areas necessary for long-term confrontation. As funding is reallocated, some of the bloated military-related industries will have to reorient themselves or shrink. This will also have consequences for global security – there will be a surplus of weapons that could be used in conflicts around the world.

Import substitution (or technological sovereignty) is one of Moscow's top

priorities and will remain so after the war. Russia has managed to find quite a few alternatives to Western technologies, doing that in a targeted manner. For example, military industry companies are required to prove that there are no alternatives on the Russian market prior to purchasing foreign components.

However, in some areas, particularly electronic components needed for high technology, Russia's dependence is enormous and long-term. Russia's modernisation requires high-precision Western-made devices and equipment, the production of which would require decades of investment. Russia is acquiring some of these technologies from China, but the Russian leadership also considers its growing dependence on China to be risky.

Although it is unlikely that Russia will catch up with the West in the field of high technology even in the long term, its technological resilience to Western sanctions is highly likely to increase in the medium term.



122 mm multiple launch
rocket system 'Grad' rocket

The Russian and Belarusian military-industrial complexes are deeply integrated and interdependent. Belarus supplies chassis for numerous Russian weapon systems, sighting equipment, optical and optoelectronic devices, radio-electronic warfare equipment, and microelectronic components. Since the start of Russia's full scale invasion of Ukraine, Belarus and Russia increased their military-technical cooperation. Belarus started supplies of components for 122 mm calibre rocket and 152 mm artillery ammunition to Russia. In the development of mass production of this type of ammunition, Belarus began construction of artillery ammunition factory in spring 2024, which is scheduled to launch operations in December 2026. Belarus obtained production lines for this factory from Russia and China. Likely, in the near term, Belarus will be able to produce artillery and rocket artillery ammunition for its domestic market and for export to Russia or other countries.

Russia increases pressure on Ukraine's supporters

Russia's objectives in its war against Ukraine remain unchanged. Despite efforts to bring Russia to peace talks and sporadic statements by its officials about their willingness to end the war,

Russia shows no desire for compromise. Russia's ongoing offensive aims at seizing as much of Ukrainian territory as possible as well as subjugating Ukraine and changing the balance of power in

Europe. Vladimir Putin likely believes that he has more will and ability to mobilise resources to achieve these goals than Ukraine and its supporters do.

As the contacts between Russia and the US intensify, European countries supporting Ukraine have become the main target in Russia's rhetoric. Russia now regards Europe, which is seeking to strengthen its defence capabilities, as a growing direct military threat and a likely major obstacle to its imperial ambitions.

Russia is increasing its hostile activities against European countries and likely is less concerned about the exposure of its covert operations and the consequences of its actions, including human casualties. It exploits these activities for propaganda purposes, using them to justify its actions, to blame NATO and the West for allegedly prolonging the war in Ukraine, to spread fear of war and chaos among European societies and cause erosion of trust in national decisions and institutions.

Russia employs measures that have a significant psychological impact using minimal resources. These actions are hard to counter, as they pursue various opportunistic objectives and are carried out by intermediaries belonging to vulnerable groups within European societies.

Not only is the Russian regime hostile towards European countries, but it also seeks to distance itself from all democratic countries. By disseminating anti-Western propaganda to domestic and international audiences, it aims to increase Russia's informational and cultural isolation. The regime firmly believes that the country would function better in a 'new' world order, cooperating with China and the Global South countries – the so-called 'global majority' – while confronting the West.

The regime retains sufficient resources to militarise the economy and society and is prepared to neutralise potential social and political instability through repression, propaganda, and long-term indoctrination.

Economic problems are unlikely to have a substantial impact on Russia's aggressive foreign policy, suggesting that Russia likely will pursue a breakthrough in its war against Ukraine in the short term. It will use all available tools to increase pressure on European countries to reduce their support for Ukraine. This will include encouraging internal divisions, threatening war, undermining the unity of European countries, and sowing discord between Europe and the US and other international partners.

The GRU is changing the methods of conducting kinetic operations and expanding the range of targets

Despite the prevention of several dozen acts of sabotage in Western countries over the past three years, the units of the Main Directorate of the General Staff of the Russian Armed Forces (GRU), which are specially trained to carry out sabotage operations and assassinations, highly likely continue to plan and coordinate operations of this nature. According to intelligence, the GRU is seeking to improve the implementation of its operations and address their chaotic execution. By using a long chain of intermediaries, the GRU is looking for more experienced individuals with criminal records willing to carry out operations for a relatively small financial reward.

The GRU is seeking to carry out more dangerous operations in Western countries, including Lithuania, by recruiting more experienced individuals. These operations could pose a greater threat to public security. In Europe, the GRU has targeted monuments that do not

align with Russia's historical narrative, as well as shopping centres, restaurants, public transportation infrastructure, and facilities related to military and humanitarian aid to Ukraine. We assess that currently, some of the GRU's main targets are individuals who support Ukraine and opponents of the Putin regime who have left Russia due to their criticism of the regime.

When planning operations, the GRU does not take into consideration the likelihood of collateral damage or damage to objects unrelated to the operation; therefore, it often uses dangerous methods of execution. This service has organised several operations in the region, using homemade incendiary devices or explosives disguised as household appliances. Thanks to successful cooperation between Lithuanian institutions and foreign partners, the planned operations have been prevented and their perpetrators arrested.

The FSB is actively conducting intelligence activities against Lithuania by regularly recruiting individuals who travel from Lithuania to Russia

At the two border control points currently operating on the border between Lithuania and the Kaliningrad Region, the Federal Security Service of the Russian Federation (FSB) is actively seeking to identify potential intelligence targets among travellers. FSB officers are taking advantage of the fact that these individuals are travelling to Russia for business or personal reasons, such as visiting relatives or dealing with property matters. The FSB considers individuals who regularly visit the Kaliningrad Region and other parts of Russia to be suitable targets, since their ability to enter the country depends on their cooperation with the FSB.

Third-country nationals residing in Lithuania are also becoming targets of the FSB; for example, lorry drivers who are employed at international logistics companies and visit Russia for work. As with Lithuanian citizens, the FSB conducts detailed interviews to determine their political views and any potential threats they pose to Russia, as well as their potential to provide intelligence. The FSB pressures third-country nationals to cooperate by threatening to ban them from entering Russia.

We assess that due to the ongoing war in Ukraine, the FSB has prioritised the collection of military and Ukraine-related intelligence. It is exploiting individuals travelling from Lithuania to Russia for collection of information on a range of subjects. These include movement of Lithuanian and NATO Allies' forces, military equipment and personnel in Lithuania, foreign troops, military exercises, the Ukrainian diaspora in Lithuania, and Lithuanian attitudes towards the war in Ukraine and support for the country. The FSB also recruits individuals who do not have access to classified information, but who can provide publicly unavailable information that the FSB is interested in.

The sanctions and restrictions imposed on Russia limit the capacity of its intelligence services to conduct human intelligence operations against Lithuania. Therefore, the FSB almost certainly will exploit every available opportunity to collect the necessary intelligence, and individuals from Lithuania who regularly visit Russia will remain a priority target for the FSB in this regard.

The FSB attempted to recruit a Lithuanian citizen who regularly travelled to Russia

After retiring from public service, Oleg*, a Lithuanian national, started a small car parts business and began to regularly visit the Kaliningrad Region for business. During the document check on his first visit to Russia, an FSB border guard discovered that Oleg often travelled to other European countries and intended to visit the region regularly. Due to his ability to provide information about his former workplace and colleagues, as well as the deployment and movement of NATO Allies' forces in Lithuania and other countries, the FSB took an interest in Oleg and decided to establish a contact with him.

The next time he was crossing the border, an FSB border guard asked Oleg to leave his car in the car park and escorted him to a separate room for an interview, where another two people in plain clothes were present. The FSB officers interacted politely with Oleg in order to assess his potential for collecting intelligence. They asked him about his previous place of employment, his colleagues and how often he visited Russia. The FSB also wanted to know about Oleg's political views and his attitude towards Russia and Lithuania's policy. During the interrogation, the FSB examined his mobile devices and collected information that could be used to characterise and/or compromise him. This included the content from his social media accounts that reflected his political views, photos, contacts in Lithuanian law enforcement and other state institutions that were of interest to the FSB. The FSB officers who conducted the interrogation decided to develop further contacts with Oleg. Knowing about his upcoming trips to the Kaliningrad Region, they decided to recruit him.

A few months later, while travelling to the Kaliningrad Region, Oleg was interviewed by FSB officers again. During the interview they asked him questions about issues of interest to the FSB, such as his contacts in Ukraine, his acquaintances among the Ukrainian community in Lithuania, his views on the 'special military operation', and any military equipment and its movement that he had observed during his stay in Lithuania. The FSB officers expressed a particular interest in information regarding other former Lithuanian officers who visited Russia. At the end of the interrogation, Oleg was offered the opportunity to 'assist Russia', with the implication that if he refused to cooperate, the FSB would prohibit Oleg from entering Russia, which would have a negative impact on his business. Oleg, having heard of similar incidents involving the FSB, reached out to the VSD, reported the interrogation and received guidance on how to handle potential recruitment attempts by Russian intelligence services.

* The name and other identifying details of the Lithuanian citizen have been changed

Intensified Russia's UAV attacks against Ukraine have led to an increase in violations of Lithuanian airspace

With Russia's massive use of UAV attacks against Ukraine's critical infrastructure, some of drones deviate from their flight paths due to technical malfunctions or the effects of EW measures and violate the airspace of neighbouring countries.

On July 10 and 28, 2025, two Russian UAVs Gerbera crashed on the territory of Lithuania. The UAV that crashed in Lithuania on July 28, had a high-explosive fragmentation charge and a navigation system with increased resistance to electronic warfare. Both UAVs entered Lithuanian airspace accidentally.

The likelihood of incidents increases due to the rising production and use of UAVs by Russia. Compared to previous years, the production of certain types of UAVs increased 2 to 10 times in 2025. Developed production capacities allowed Russia to increase the scale of UAV strikes against Ukraine from approximately 300 in early 2024 to more than 6,000 in July 2025. The production of long-range UAVs (Geran-2 and Gerbera types) increased from 500 units in 2024 to 5,000-6,000 units a month in 2025.



UAV and combat ammunition found after the crashes in Lithuania on July 10 and 28. Images by Lithuanian Armed Forces and Defence Intelligence and Security Service

It is highly likely that the situation in the Baltic Sea will remain tense – Russia is determined to protect its commercial interests by any means necessary

International sanctions against Russia's shadow fleet have disrupted Russia's strategy and reduced the profits Russian companies derive from trading in energy resources. However, a large part of the shadow fleet still uses the Baltic Sea route to export oil and oil products, accounting for 40 percent of Russian oil exports by sea.

Russia's shadow fleet consists of up to 1,000 ships worldwide, transporting Russian oil and liquefied gas. This is an important tool for Russia to sell raw materials, bypassing the price cap set by sanctions and thus securing additional revenue needed to finance the war against Ukraine.

Crews of these ships seek to conceal the origin of their cargo by turning off Automatic Identification System or manipulating data by transmitting false location coordinates. Other evasion tactics, such as transferring cargo from ship to ship on the high seas, pose environmental risks. Complex ownership and management structures are used to conceal true owners of the tankers.

Russia has taken additional measures to ensure an uninterrupted operation of its shadow fleet in the Baltic Sea. It is almost certain that for Russia to not allow Western authorities to inspect its shadow fleet tankers or their crews is of utmost importance. It is highly likely that Russia is determined to use military means to achieve this. There are increasing cases of more aggressive displays of force, including unsafe manoeuvres near NATO military ships and aircraft. In 2025, shadow fleet tankers in the Baltic Sea were accompanied not only by Russian warships but also by its Su-35S and Su-30SM fighter jets, which were taking risks and violating the airspace of NATO countries. For example, in May 2025, a Russian Su-35S multi-role fighter violated Estonian airspace while escorting an unflagged tanker Jaguar, subject to international sanctions. Russia's aggressive behaviour in protecting its shadow fleet tankers increases the risk of incidents in the Baltic Sea.

Although ship incidents in the Baltic Sea in 2023–2025 involving damage

to strategically important underwater infrastructure are not linked to deliberate actions by crews of ships calling at Russian seaports, the infrastructure stretching across the Baltic Sea remains

vulnerable. Incidents caused by a combination of circumstances, such as poor weather conditions, technical defects in ships, and irresponsible attitudes towards navigation, are possible.

Russia rather adapts to an economic slowdown than changes its military ambitions

The Kremlin justifies the transfer of military costs to Russian citizens as necessary for national survival, given the 'fateful war' taking place around Russia. Despite the deteriorating economic situation, Russia's defence and national security spending will remain at record levels in 2026-2028, accounting for about 38 percent of the total budget, or 7-8 percent of GDP. Russia is currently mobilising its economic resources primarily to continue its aggression against Ukraine; but even if the war in Ukraine ends, the restoration of arms reserves and the development of the Armed Forces will remain key priorities in the medium and long term.

The militarisation of the Russian economy has exacerbated structural problems. State investment in the military

industry does not provide a basis for sustainable economic development. Having ensured growth in 2023-2024, further development is hampered by the limits of state needs, labour shortages, and ongoing supply chain and raw material constraints. Russian regions involved in military industry activities are maintaining annual economic growth, but other regions are showing clear signs of economic stagnation or even decline.

The Kremlin is promoting the narrative that Russia's economic situation allows it to continue the war against Ukraine and that the country's economy can develop despite the sanctions imposed by Western countries. The uncontrollable inflation, growing budget deficit and rapidly declining volume of liquid

assets of the National Welfare Fund became the most prominent signs of Russia's ineffective fiscal policy in 2025. Despite Putin's promise to the public not to raise taxes until 2030, Russian citizens welcomed the New Year with an even greater burden of new or adjusted taxes: firstly, with an increased value-added tax (VAT) and more entities and individuals as tax payers. It is unlikely that deteriorating living standards will pose a risk to the Kremlin's political stability. Low unemployment, nominal wage growth, and high demand for labour in

the defence sector have so far directly cushioned the effect of the economic slowdown on society.

Since the start of the war against Ukraine, Russia's economic model has exhausted its capacity and macroeconomic indicators are deteriorating, but even if the economic situation continues to worsen, military spending will remain a priority for the Kremlin. Russia's determination to strengthen its military power remains a major source of threat to its neighbours.



Elvira Nabiullina is the Chairwoman of the Central Bank of Russia, which is responsible for the financial stability but powerless against the Kremlin's political decisions.

ZUMA / Press photo

During the strategic exercise Zapad 2025 Russia applied lessons learned in Ukraine

The Russian-Belarusian strategic military exercise Zapad 2025, held in August-September 2025, was smaller in scale than previously due to the Russian Armed Forces' involvement in combat operations against Ukraine. Up to 30,000 Russian and Belarusian military personnel took part in the exercise, as well as a small number of foreign military personnel and observers.

During the exercise Russia sought to demonstrate its ability to carry out a normal military training cycle and modernise its Armed Forces even while engaged in the large-scale war against Ukraine. It is highly likely that for the sake of deterrence and demonstration of power, Putin stated that 100,000 soldiers had participated in the exercise – several times more than the actual number. Russia's political and military leadership also emphasised the country's technological advances during the exercise, showcasing unmanned and robotic technology and electronic warfare capabilities.

The official training scenario included joint Russian and Belarussian defence actions of the Union State against the external aggressor. In fact, the exercise

simulated a military conflict with NATO and tested the readiness of the Russian Armed Forces to fight in such a conflict. Like Moscow, Belarus in its rhetoric emphasised the defensive nature of the Zapad exercise, designed to prepare for a counterattack in the event of aggression and accused neighbouring NATO countries of militarisation. The Belarusian regime highlighted the increase in military contingents in the Baltic States and Poland, the number and scale of exercises with NATO allies, and raised assumptions about the allegedly aggressive intentions of NATO countries towards Belarus.

Even before the start of the exercise, Belarusian political and military leaders publicised their decision to reduce the scale of Zapad and move the training sites away from the western borders. However, they later acknowledged that the Belarusian Armed Forces would be active in the border areas during the exercise.

Exercise-related military activity in the vicinity of Lithuania – in the Kaliningrad Region and Belarus – was significantly smaller in scale than during the previous Zapad exercises.

The main focus of the Zapad 2025 exercise was on integrating the lessons learned from the war against Ukraine: forming assault units specialising in capturing fortified defensive positions and strongpoints; camouflage, setting up engineering positions; logistics dispersal; the use of large numbers of UAVs in offensive and defensive operations.

- **Logistics dispersal tactics.** Larger logistics supply points are moved away a safe distance from the front line, resources are delivered by trucks and are not concentrated in one area. In some cases, horses or donkeys are used to supply units, and supply routes are covered with nets that provide protection from drone attacks.
- **UAV innovations.** FPV (first-person view) type UAVs with optical cables are used; they are resistant to the effects of EW measures, operate at a distance of up to 40 km, and can be used to attack logistics lines and points. Russia also uses this type of UAVs with solar batteries, which extend their operating time.
- **Development of anti-drone measures.** Various portable or vehicle-mounted signal jamming systems, directional electronic countermeasures, or real-time radio-electronic spectrum analysers are used to detect approaching UAVs.

Moscow tries to intimidate the West by creating the myth of the invincible Oreshnik missile

Russia is conducting a propaganda campaign related to the development of the Oreshnik intermediate-range ballistic missile, emphasising the missile's striking power and thus seeking to inflate the capabilities of its military

industry. At the end of 2024, Russia's Armed Forces used an intermediate-range ballistic missile for the first time in the war against Ukraine, which Putin described as a completely new hypersonic missile called the Oreshnik.

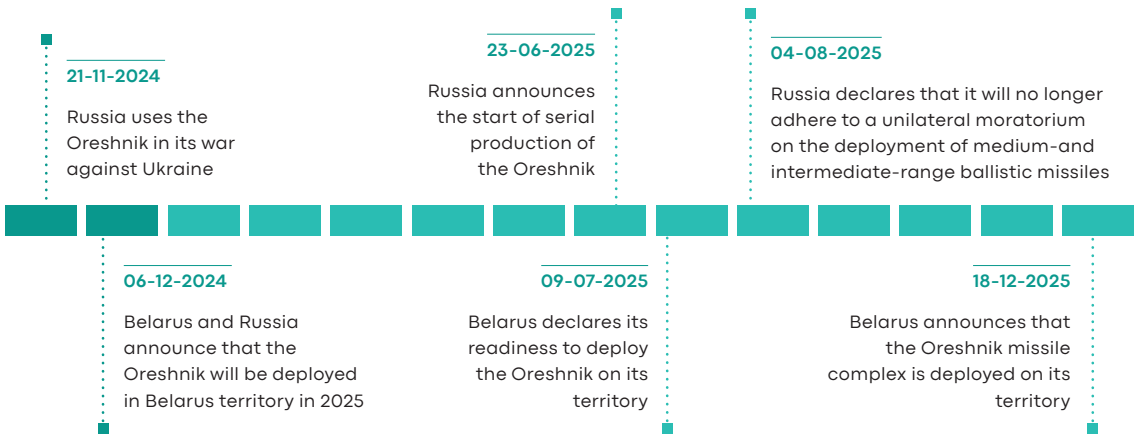
Russia's public communication about its development is intended to pressure the West to reduce its support for Ukraine and Kyiv, and to refrain from decisive actions against Russian aggression.

One of the most important elements of the communication about the Oreshnik is a public announcement of Oreshnik deployment in Belarus in December 2025. Russia presents this decision as a response to the US plans to deploy the Typhon ground-based missile system

in Germany on an episodic basis from 2026. However, the deployment of the Oreshnik in Belarus will not significantly impact the security of Lithuania, as the missile range is already sufficient to reach targets in our region from Russian territory.

The Oreshnik missile complex deployed in Belarus belongs to Russia's strategic missile forces, so Russia will retain full control over it and gain another lever in its relations with Minsk.

Events related to Oreshnik missile



Despite the collapse of Bashar al-Assad's regime, Russia will maintain its military capabilities in Syria

Even after the regime change in Damascus, Russia retained part of its military capabilities in Syria, as relations between the two countries remained based on mutually beneficial pragmatic interests. Moscow seeks to maintain at least part of its military capabilities at the Tartus naval base and Khmeimim airbase, as these military facilities are important for ensuring logistics for Russian operations on the African continent and the activities of the Russian Navy in the Mediterranean Sea.

In 2024, following the collapse of Bashar al-Assad's regime, Russia had to withdraw some of its forces and military

equipment from the country. However, the Kremlin soon began negotiations with Hay'at Tahrir al-Sham (HTS), the group that took power in Syria, on maintaining its forces in Syria. Although HTS initially declared a critical stance towards relations with Russia due to its support for the Assad regime, the two sides subsequently held several rounds of negotiations, and Putin eventually received Syrian President Ahmed al Sharaa at the Kremlin. Although on a much smaller scale than during Bashar al-Assad's rule, it is highly likely that Russia will maintain its military presence in Syria in the near term.



Russia expands its activities in Africa to maintain its image as a global power

Africa is important to Russia as part of Moscow's global southern policy, in reducing its international isolation and counterbalancing its lost Western markets. Russia uses political advisers, intelligence services, economic deals, the Orthodox Church, military support and cultural exchanges to expand its influence in Africa. In 2025, the Russian presidential administration established the Strategic Partnership and Cooperation Department, which is also responsible for cooperation with the African continent, demonstrating the desire to pursue a consistent, coordinated policy and make more effective use of the resources allocated for this purpose.

Russia has interests in all African regions, but most recently it has concentrated on the West African coast, where it seeks access to ports as well as mineral resources and provides support for the political Sahel Alliance project. Cooperation with African countries allows Moscow to secure income from the extraction of natural resources, to spread its propaganda narratives and maintain its image of power. One of the most important directions of Russia's activities in Africa is cooperation in the areas of security, military and arms supplies.

Activities of the Africa Corps

The Russian Ministry of Defence continues its efforts to consolidate military influence on the African continent through its military organisation, the Africa Corps. In order to expand the Corps' activities, Russia offers its personnel high salaries, similar to those of soldiers sent to fight against Ukraine. The Africa Corps is currently involved in combat operations in Mali and is performing various tasks in Burkina Faso, Libya, Niger, and Equatorial Guinea, such as training local soldiers and protecting VIPs and strategic objects. However, in 2025, the Africa Corps failed to replace Wagner in the Central African Republic.

A larger-scale expansion of the Africa Corps is unlikely in the near term, partly due to limited interest of African countries. However, once the large-scale war against Ukraine ends or fighting on the front lines ceases, it cannot be ruled out that Russia could use some of the troops, weapons, and other freed-up resources to expand its operations in Africa.



BELARUS

- **Although the Belarusian regime has expressed an interest in improving relations with Western countries, it almost certainly does not intend to soften its authoritarian policies.** Public meetings between Alexander Lukashenka and Western officials strengthen the international status of the Belarusian regime. The regime uses these meetings in its propaganda to reinforce the narrative that ensuring regional security is inseparable from Belarus's involvement in addressing security issues in the region.
- **Easing sanctions against Belarus is likely to have a significant impact on the country's economic sustainability and growth.** However, restoring economic ties with the West will not offset Belarus's growing economic dependence on Russia.
- **In its fight against political opponents, the Belarusian regime compiles extremist watchlists that include members of the political opposition, as well as anyone who criticises the regime – including individuals and entities from other countries.** Anyone who is on the lists or has connections with those included faces the threat of arrest in Belarus.
- **Cooperation with China is becoming increasingly important for the Belarusian economy.** To further this economic partnership, Belarus is showing greater support for China's foreign policy and strengthening security ties.

Lukashenka is easing international isolation of the Belarusian regime but does not abandon authoritarian practices or the country's orientation towards Russia

After more than five years of international isolation of the Belarusian regime, Lukashenka highly likely believes that the changing foreign policy landscape presents an opportunity to restore Belarus's relations with the West to their pre-2020 state.

Although the Belarusian regime has expressed an interest in improving relations with Western countries, it almost certainly does not intend to soften its authoritarian policies. Lukashenka is maintaining his grip on power through repressive measures; therefore, in the medium term, the regime will continue to persecute opponents, critics and even individuals seeking alternative information. By releasing prominent Belarusian democratic opposition figures and other political prisoners, the Belarusian regime almost certainly was primarily hoping for a favourable response and proposals for possible negotiations from

Western countries or the lifting of sanctions. Using political prisoners as a bargaining tool is an age-old tactic of the Belarusian regime, as demonstrated multiple times in the past when political prisoners were released in order to demonstrate the regime's alleged goodwill.

The regime is seeking to restore relations or soften sanctions not only by releasing political prisoners. It is also pursuing these objectives by creating or exploiting problems that threaten the security of neighbouring countries. While we assess that the regime has the capability to prevent the smuggling of cigarettes by high-altitude balloons, it deliberately exploits this criminal activity for political gain – specifically to initiate a political dialogue with Lithuania and reduce the restrictions imposed on Belarus. As was the case in 2021, when it orchestrated an illegal

migration crisis, the regime is claiming that the balloon crisis cannot be resolved due to international sanctions imposed on the country or unwillingness of Belarus's supposedly hostile neighbours to cooperate.

The Belarusian regime's attempts to normalise relations with the West are motivated by political and economic interests. Proving the legitimacy of his rule is essential to Lukashenka. His public meetings with Western officials strengthen Belarusian regime's international status and create the impression that it is no longer as isolated as it was following its crackdown on protests against rigging of the 2020 presidential election. The regime's propaganda exploits Lukashenka's contacts with Western representatives for both domestic and foreign policy gains, reinforcing the narrative that ensuring regional security is inseparable from Belarus's involvement in addressing security problems in the region.

Although the regime denies the impact of Western sanctions on the Belaru-

sian economy, the easing of the sanctions on key economic sectors is likely to have a significant impact on the country's economic sustainability and growth. At present, Belarus's economic stability is only ensured by continued financial support from Russia, the most significant factor contributing to the country's dependency on Russia. While restoring economic ties with the West would partially reduce the economic pressure on Belarus, it would not constitute an alternative to its growing economic dependence on Russia.

Despite Belarus's interest in improving relations with the West, its policies and actions towards Lithuania and neighbouring countries are highly likely to remain aggressive in the near term. While Belarus is likely to convey its desire to restore relations and cooperation with Lithuania, it will be reluctant to take concrete steps to reduce tensions. It will deny any involvement in hostile actions against Lithuania and will disseminate propaganda accusing Lithuania of aggression towards Belarus.



Lukashenka meets with US Special Envoy for Belarus John Coale in Minsk.
AFP photo

Relations with China help Belarus to reduce the impact of international isolation

In recent years, the Belarusian regime has been making significant efforts to strengthen its cooperation with China due to international sanctions and isolation. Minsk is keen on attracting more Chinese investment, expanding bilateral trade, and developing the Great Stone industrial park, as well as strengthening ties in technology and infrastructure development. The representatives of Belarusian and Chinese governments hold regular meetings at various levels to discuss opportunities for cooperation in these areas.

Although economic cooperation with China is becoming increasingly important for Belarus, China is becoming more cautious in this area. Over the past five years, direct investment in Belarus has declined significantly, as China has shifted towards safer forms of financial cooperation, such as loans. Bilateral trade is growing, but the trade balance is significantly more favourable to China.

Belarus's increasing support for China's foreign policy and deepening ties in security cooperation in exchange for economic partnership is a noticeable trend. Cooperation in the security field between the countries is likely to pose challenges in the region, as they will encourage closer collaboration between Chinese and Belarusian intelligence services and create favourable conditions for the Minsk regime to strengthen its control over Belarusian society and the country's security apparatus.

Russia is almost certain to remain tolerant of these ties as long as they serve its interests in the context of the war in Ukraine. Russia highly likely is leveraging the ties between Belarus and China to procure sanctioned items and mitigate the impact of restrictions on its economy. China highly likely prioritises maintaining good relations with Russia and therefore does not seek to challenge its influence in Belarus.

Belarus's use of extremist watchlists and remote recruitment of agents in its fight against the democratic opposition poses a threat to Lithuania

The Belarusian regime constantly adapts its tactics to counter political opponents and their supporters, as well as neighbouring countries and their citizens who criticise the regime's illegal actions. The regime uses extremist watchlists that include anyone involved in opposition activities or in criticising Lukashenka and his policies. These watchlists are aimed at not only combatting opponents but also intimidating and controlling society. Since 2020, the majority of individuals added to the lists have been convicted on political grounds of criticising the regime or having links to the Belarusian democratic opposition. Hundreds of individuals, organisations and other entities are added to the list every month. These not only include individuals and entities from Belarus but also from foreign countries, such as Lithuania, who criticise the Belarusian regime and express support for the democratic opposition. In July 2025, the Russian-language Delfi

Litva YouTube channel, which has over 100,000 subscribers, was designated as extremist in Belarus. This was likely due to a published interview with Siarhei Tsikhanouski, a representative of the Belarusian democratic opposition. Subscribers to this channel are likely to face administrative arrest when travelling to Belarus.

The Belarusian State Security Committee (KGB) conducts interviews and checks on individuals travelling from Lithuania to Belarus, including inspection of their mobile devices. In search of information relevant to Belarusian intelligence, KGB officers look for links to organisations and references to online sources that have been declared extremist, including evidence of subscriptions to them. The Belarusian regime considers even distant links to such entities as sufficient grounds for detaining individuals, arresting them, and adding them to extremist watchlists.

In August 2024, a Lithuanian citizen was detained and imprisoned in Belarus. He was the administrator of social media channels that criticised the Belarusian regime and were added to the extremist watchlists in 2022. During his period of incarceration, the Lithuanian citizen was subjected to constant psychological pressure by the KGB. He underwent a polygraph test and was interrogated on multiple occasions. During the imprisonment, he was threatened that if he refused to comply with the KGB's orders, his wife would be detained and charged with colluding with Lithuanian intelligence, and their children would be placed into foster care.

The KGB pressured the Lithuanian citizen to participate in propaganda interviews that portrayed the Belarusian regime positively, to appear in videos that discredited Lithuania, and make phone calls to Lithuanian institutions. During the calls, representatives of Lithuanian institutions were provoked to comment on Lithuanian-Belarusian relations. It is highly likely that the KGB planned to use recordings of these calls for propaganda activities against Lithuania. The videos were intended to discredit the deployment of NATO troops in Lithuania, portray Lithuanian institutions negatively, and present the Belarusian regime positively.

Not only does the Belarusian regime resort to the intimidation by using extremist watchlists to counter the democratic opposition and repress political opponents. Belarusian intelligence also recruits members of the diaspora residing in Lithuania to gather information on the diaspora, the democratic opposition and their activities. The KGB has been increasingly recruiting agents among Belarusians living in Lithuania via messaging apps. In return

for information, the KGB offers financial payments, the opportunity to obtain a newly issued passport and the freedom to visit Belarus, as well as safety for those who return to live there. The KGB also blackmails the recruited members of the diaspora. Those who refuse to cooperate are subjected to psychological pressure, primarily by threatening to confiscate their property in Belarus and endanger the safety of relatives who remain there.



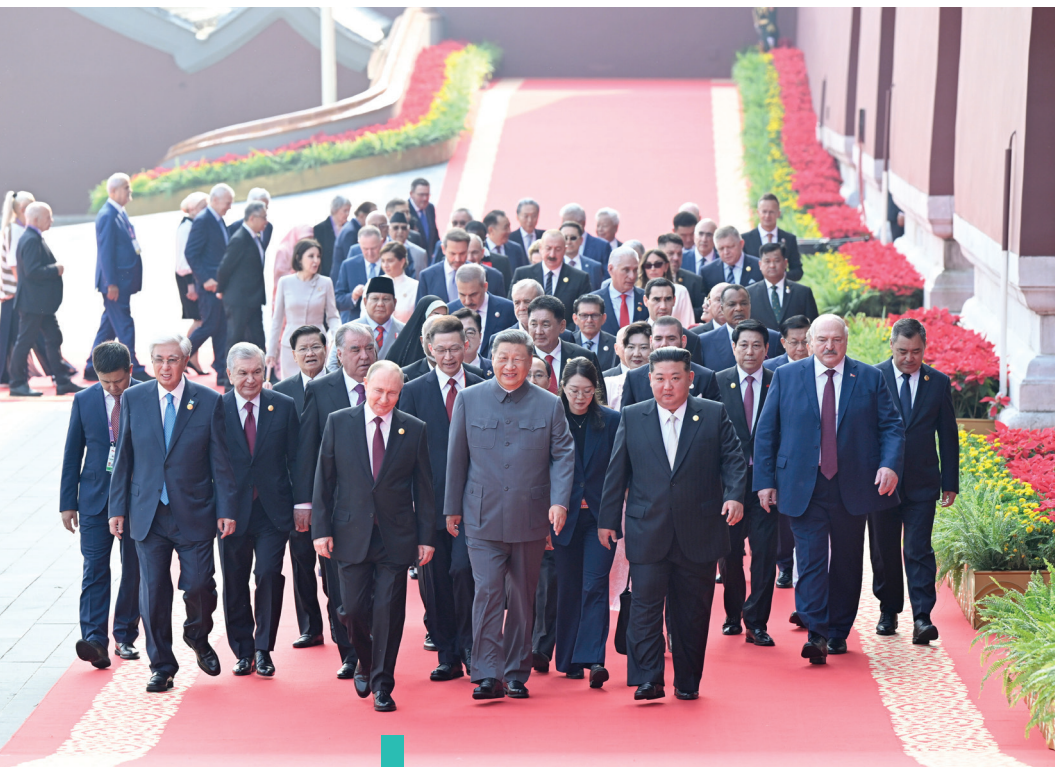
CHINA

- **China is increasingly presenting itself as leader of a group of countries that are questioning the current international system.** By uniting authoritarian states and playing an active role in international organisations, China is seeking to decouple from Western institutions, financial systems and supply chains while advancing its foreign and security policy goals.
- **China is rapidly strengthening its military power by consistently increasing its defence budget and investing in modern military capabilities.**
- **Dominance in the East and South China Seas and around Taiwan remains China's key strategic priority.** In recent years, the Chinese People's Liberation Army (PLA) has also been expanding its overseas maritime operations and conducting exercises beyond its usual areas of operation. This demonstrates the country's growing ability to project military power globally in order to secure its interests and influence.
- **China is strengthening its strategic partnership with Russia.** The main goal of joint military activities is to express political support for each other and demonstrate military power. Joint military exercises and patrols in the Indian and Pacific Oceans increase pressure on NATO allies and partner countries.

China seeks to reshape the international order by forming a bloc of anti-Western states

China is increasingly presenting itself as leader of a bloc of countries that question the current international system. Alongside Russia, North Korea and Iran, China believes that the post-Cold War international order needs reshaping because it no longer reflects current geopolitical realities and serves the interests of the West, particularly the US.

China is not only bringing together countries hostile to the West by inviting their leaders to participate in Chinese-organised military parades or forums, it is also collaborating with them in international organisations. This approach helps to form opposition to the West and strengthens China's strategic interests, enhances its global



Foreign leaders during the military parade in Beijing in September 2025.

EPA photo

influence. China plays an active role in the United Nations (UN), the BRICS group and the Shanghai Cooperation Organisation (SCO).

China officially declares its support for the rules enshrined in the UN Charter, but at the same time it is actively seeking to change the organisation from within. It is making great efforts to have its representatives appointed to senior positions in UN agencies with significant financial resources that can be exploited for its interests. China aims to turn its national initiatives, such as infrastructure development and technology standardisation, into the official goals of the entire organisation, and seeks to implement them using shared resources.

At the UN level, China is actively forming coalitions with authoritarian and developing countries. These countries support China by voting unanimously in the General Assembly on issues important to China and help it to shape the activities of UN agencies in a favourable direction. This allows China to establish a significant counterweight to the West on matters such as human rights, Taiwan, and the resolution of international conflicts.

China's stance on the Russian war against Ukraine highlights clear differences between its stated principals and its actions within the UN. Although China emphasises its respect for UN principles such as state sovereignty and territorial integrity, it abstains from or votes against resolutions condemning Russia's invasion because it considers Moscow to be a strategic partner. At the same time, China promotes its own vision for peace in Ukraine at the UN. After securing support from developing and authoritarian states, it positions itself as a neutral actor committed to peace.

China is also expanding its influence within the BRICS group. Being a strong advocate for the organisation's expansion, China prioritises the accession of countries that it has established close bilateral relations with. Following China's initiative, a special BRICS partner status has been granted to ten countries, including Belarus and Kazakhstan, as well as countries in Latin America, Africa, and Southeast Asia.

China uses an anti-colonialist narrative to unite countries within the BRICS organisation. It argues that the world order established by the West is

founded on inequality and exploitation, and that it can help to ensure a fairer representation. China is expanding its influence by using the BRICS Development Bank, established in Shanghai. It encourages members of the organisation to actively participate in Belt and Road Initiative projects, to use the yuan for international financial transactions and establish financial systems independent of those of the West.

China is increasingly expanding its influence within the SCO, broadening the organisation's scope and mandate. As with the BRICS, China favours the expansion of the organisation, which would extend the SCO's influence beyond Central Asia. Belarus and Iran have recently become members of the organisation, and another 14 countries from the Middle East, North Africa and Southeast Asia participate in its activities as partners.

At the SCO summit in September 2025, China announced the Global Governance Initiative, which emphasises the importance of a multipolar world. This initiative also underlines the need to establish and strengthen platforms for

economic, energy, technological, and security cooperation independent of the West. The meeting also approved Beijing's initiative to establish the SCO Development Bank, which China is highly likely to use to bolster its influence within the organisation. China is also seeking to expand the scope of the SCO to include issues that are relevant to its national interests, such as renewable energy, technological innovation, and security challenges.

In the medium term, China's role in uniting and strengthening the anti-Western bloc almost certainly will pose an increasing challenge to the security interests of Lithuania and its allies in the Euro-Atlantic region. The establishment of such a bloc will enable China to decouple from Western institutions, financial systems and supply chains, while furthering its foreign and security policy objectives. This highly likely will increase China's resilience, enabling it to pursue its geopolitical goals more aggressively in the Indo-Pacific region and on a global scale. It will also create favourable conditions for other states close to China to pursue their own revisionist goals.

The use of Chinese artificial intelligence chatbots presents challenges in terms of personal data security and information censorship

The Chinese artificial intelligence (AI) chatbots, DeepSeek and Qwen, are being promoted as alternatives to Western AI models, such as ChatGPT. While this demonstrates China's ambition and capability to compete with the West, it also poses challenges for users in terms of information censorship and personal data security when using these chatbots.

INFORMATION CENSORSHIP

Both chatbots provide users with information that is consistent with the regime's ideology, avoiding responses that would portray China negatively. For example, they avoid discussing Taiwanese independence or the Tiananmen Square protests. DeepSeek repeats the statements of Chinese politicians and uses the pronoun 'we' when answering questions about China's position to show its identification with China.

In February 2025, *Politico* published a chat with DeepSeek asking why China had blocked imports of goods from Lithuania. The chatbot expressed hope that Lithuania would correct its mistakes and cooperate with China. This response essentially echoed the call made by the Chinese Ministry of Foreign Affairs spokesperson Wang Wenbin in 2023 for Lithuania to 'correct its mistakes and return to the right path by supporting the one-China principle'. Such responses, alongside with the nature of Chinese chatbots, suggest that biased information is presented to users.

PERSONAL DATA SECURITY

DeepSeek collects the following types of information: data created by users themselves, such as query texts and various documents shared with the chatbot; automatically accessible information, such as device data and IP address; third-party data, such as information linked to a Google account.

According to Chinese law, the government is entitled to access data collected by technology companies. Chinese-developed AI software possibly lacks adequate cybersecurity measures necessary to protect the user data. Shortly after its launch, more than a million pieces of data collected by the DeepSeek chatbot were leaked, including chat system metadata and chat transcripts.



DeepSeek and Qwen logos
Reuters photo

Timeline of China's military power projection

2022

Xi and Putin announce an 'unlimited strategic partnership'. After Russia launches a large-scale invasion of Ukraine, Beijing does not condemn Moscow, publicly declares neutrality, and begins to increase cooperation with Russia.

Although on a smaller scale than before, China participates in Russia's Vostok 2022 military exercises.

In response to the Speaker of US House of Representatives Nancy Pelosi's visit to Taiwan, China conducts large-scale military exercises around the island.

2016

China loses a case against the Philippines at the Permanent Court of Arbitration in the Hague over a dispute over territories in the South China Sea. China's refusal to recognise the court's unfavourable ruling, along with both countries' desire to control their respective territories, continues to cause incidents in the South China Sea.

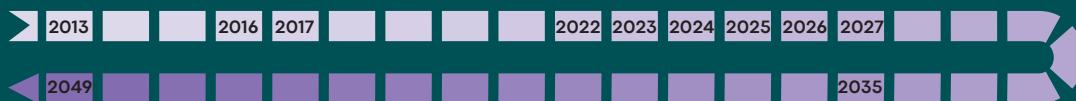
2017

Xi Jinping announces an ambitious plan to modernise the Chinese military, and China's first overseas military base is established in Djibouti.

For the first time, a *PLA ship arrives to celebrate the Russian Navy Day in the Baltic Sea.

2013

China begins constructing artificial islands in the South China Sea, later militarising them.



2023

In response to unfavourable results of the parliamentary and presidential elections in Taiwan, China once again conducts large-scale military exercises around the island and intensifies pressure through other non-military means.

2024

China and Belarus hold joint, mostly symbolic, anti-terrorist exercises, Eagle Assault, in Brest, which have been held periodically since 2011.

Two Chinese ships navigate the Baltic Sea and participate in small-scale Russian military exercises in the Gulf of Finland.

China and Russia conduct joint air and sea patrols in remote parts of the Pacific Ocean, demonstrating their growing military partnership.

2025

At the beginning of the year, a Chinese naval fleet sails around Australia and conducts live-fire exercises in international waters.

China does not participate in the Zapad 2025 military exercises held by Russia and Belarus close to Europe, and sends only observers.

2026

China continues to project military power into the western Pacific, seeks opportunities to gain new leverage in other regions, and maintains close military ties with Russia.

by 2027

Xi has set a goal for the Chinese military to acquire capabilities that would allow it to reunite Taiwan with mainland China.

by 2035

The aim to complete the modernisation of the PLA, bringing it closer to the world's most powerful armies.

by 2049

China aims to have 'world-class' military.

* Chinese People's Liberation Army.

China is consistently increasing its military power in order to ensure its security interests and expand its influence

Beijing's goal is to develop an army capable of winning wars against its most powerful rivals and their allies by 2049, the 100th anniversary of founding the People's Republic of China. Despite the slowing economy and related social and other challenges within the country, China is steadily increasing its defence budget every year. Beijing is prioritising the modernisation of its Armed Forces, investing heavily in the construction of new aircraft carriers and amphibious assault ships, and strengthening its Rocket Force and Air Force. China's growing military power in the Indian and Pacific Oceans poses challenges to the economic and security interests of NATO allies and partners, as well as freedom of navigation, and increases tensions in the region.

Reunification with Taiwan remains a key strategic goal for China. In recent years, Beijing has stepped up political, military and information pressure on Taipei in order to implement its One China Principle and deter the island from any independence aspirations. The rhetoric of senior Chinese Commu-

nist Party officials towards Taiwan has also become more aggressive, including direct threats of military conflict.

During exercises held in the spring of 2025, in addition to the usual blockade manoeuvres, China's forces simulated strikes on Taiwan's defence and energy infrastructure and trained to block strategic supply corridors. At the end of 2025, China held another unannounced exercise around Taiwan to warn its potential foreign allies. Compared to previous exercises, these were larger in scope and took place closer to Taiwan, featuring the deployment of more advanced amphibious ships and significant aviation activity. In addition to deterrence, the Chinese military leadership's goal is to gain experience, to exhaust the Taiwanese military, and reduce Taipei's alertness by normalising constant military activity around the island.

China seeks to establish dominance in the South China Sea and uses various means to disrupt movement and aggressively demonstrate control over



The Chinese People's Liberation Army Navy (PLAN) Jiangkai-class frigate Hengyang was spotted by Australian defence forces. On February 21, 2025, Australian Foreign Minister Penny Wong expressed concern about three Chinese warships conducting live-fire exercises off the country's east coast.
AFP photo

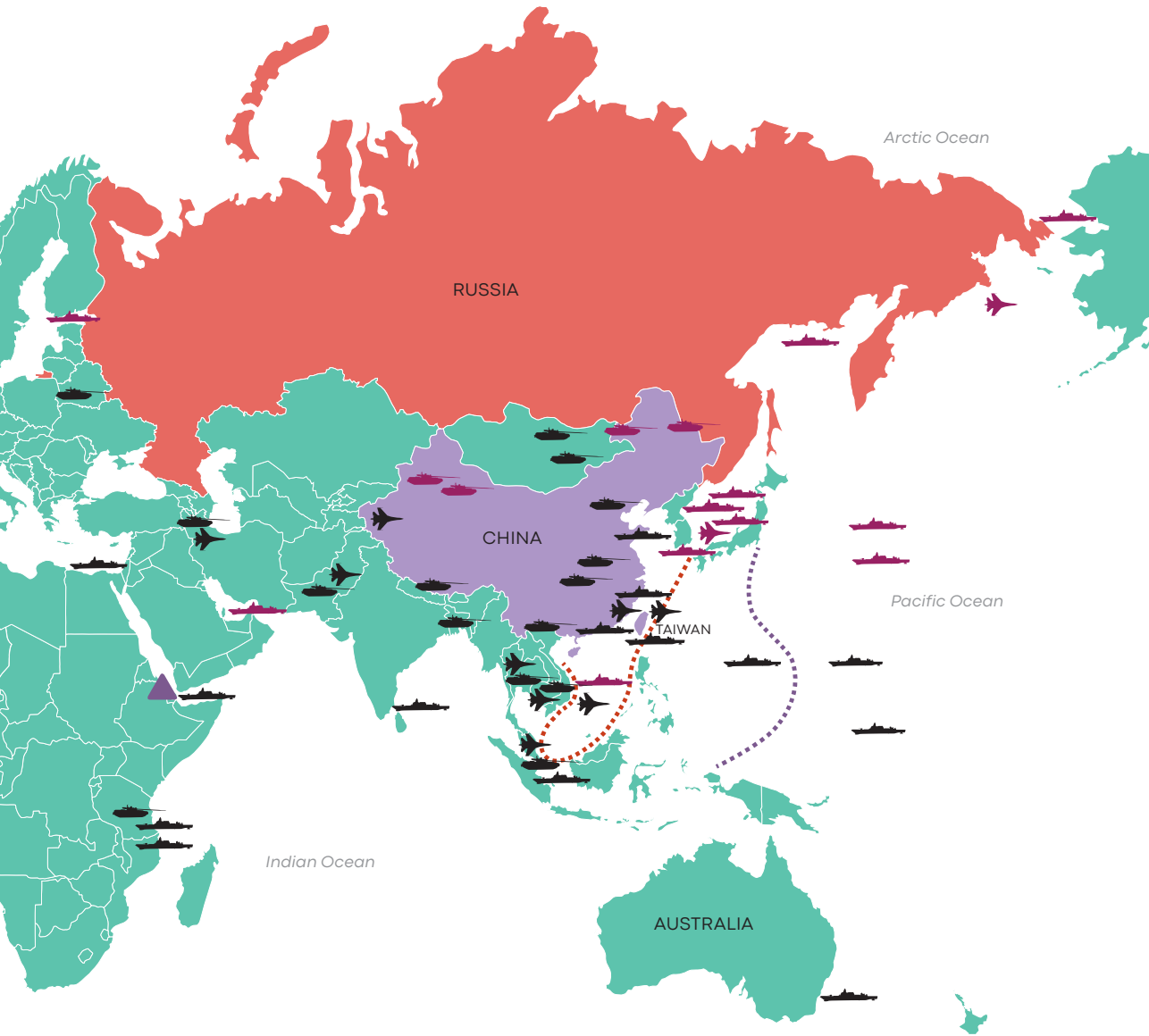
the territories it has claimed, including the militarisation of islands. In 2024–2025, tensions between China and the Philippines grew over strategically important and resource-rich parts of the South China Sea. Chinese Coast Guard vessels in the South China Sea, especially near the Spratly Islands, regularly carried out dangerous blocking and ramming manoeuvres, as well as using water cannons against Philippine vessels. Such incidents significantly increase the likelihood of unintentional military incidents and escalate the security situation in the region.

In addition, the so-called far-sea operations further away from China's shores are being carried out more actively: in early 2025, a Chinese naval fleet sailed around Australia and conducted live-

fire exercises in international waters. This operation was the southernmost mission of the Chinese Navy. In June 2025, two Chinese aircraft carriers and accompanying military ships navigated together for the first time near the second island chain in the Pacific Ocean.

In this regard, China is not only sending a message about the naval dominance in the region and seeking to deter third countries from interfering in a possible military conflict with Taiwan, but also demonstrating its dissatisfaction with the US, Japan and South Korea's military partnership in the Pacific Ocean, and the pro-Western regional security formats QUAD and AUKUS. It is likely that the scale and geography of such Chinese operations will expand in the future.

China's military power projection in 2024-2025



..... 1st island chain

..... 2nd island chain

▲ China's army support base in Djibouti

Joint military exercises and / or patrols by the PRC and the RF

 Navy

 Air Force

 Ground Force

Other PRC unilateral / bilateral / multilateral exercises and / or patrols

 Navy

 Air Force

 Ground Force

NOTE: Only the majority of the most important events are listed, and their locations are approximate.

Intensifying military cooperation between Russia and China signals a strengthening strategic partnership

Joint Chinese and Russian military exercises and patrols continued even as Russia is still at war with Ukraine. In recent years, joint military manoeuvres started being held not only in the South China Sea but also in the Arctic region. The exercises have often been carried out near Japan, South Korea, the Philippines and Alaska, significantly increasing pressure on the US and NATO partners in the region.

By allowing Chinese military ships to enter its Arctic territories, Russia is likely making concessions to Beijing and revising its previous policy of restricting China's military activity in the northern regions of the country in return for China's support during Russia's war

against Ukraine. It is almost certain that China is seeking to establish a long-term military presence in the region.

In joint military drills, the Chinese army is learning from the experience gained by Russia in its war against Ukraine, while Moscow, with Beijing's support, has showed that Russia is not isolated and can challenge Western dominance on several fronts at once.

Joint military exercises and patrols in the Indian and Pacific Oceans demonstrate the growing strategic partnership between Beijing and Moscow aimed at deterring opponents — especially the US and its allies — and changing the regional security architecture.

The most significant joint Chinese-Russian military manoeuvres in 2024-2025:

- In July 2024, the first joint patrol by Chinese and Russian military Air Forces was observed near the coast of Alaska.
- In October 2024, Chinese Coast Guard ships patrolling with Russian forces entered the Arctic Ocean for the first time.
- In August 2025, joint submarine patrol was conducted for the first time in the seas of Japan and East China.



Farewell ceremony in Vladivostok for Chinese and Russian military ships leaving to participate in joint naval and air force exercises 'Northern / Interaction-2024' in the seas of Japan and Okhotsk.
IMAGO / SNA photo

ECONOMIC AND ENERGY SECURITY

■ **Belarus is committed to developing nuclear energy near the Lithuanian border by constructing a third unit at the Belarussian Nuclear Power Plant.** However, the implementation of this project is not economically viable given that the power plant is currently not operating at full capacity. Developing nuclear energy in Belarus will pose a risk to Lithuanian and regional security, as Belarus will be unable to ensure the safety of the new project, and attention will be distracted from incidents at the currently operational nuclear power plant.

■ **Companies with links to Russia and Belarus, as well as individual citizens of these countries, are showing interest in Lithuania's transport, energy and high-tech sectors.** To gain access to sectors or infrastructure of strategic importance, they establish business contacts with entrepreneurs from other European countries or the US, using them as intermediaries to avoid direct participation in business ventures.

■ **Russia and Belarus are seeking to acquire and further develop Western dual-use technologies via companies based in other countries.** Their interests in obtaining Western technologies will remain particularly high, since they are unlikely to achieve technological sovereignty in the near term despite their efforts to reduce their dependence on Western technologies.

Belarus is committed to the development of nuclear energy in the vicinity of the Lithuanian border

The Belarusian government is determined to build a third unit at the Belarusian Nuclear Power Plant (NPP), in addition to the existing two units. It justifies the construction of Unit 3 on the basis of the country's allegedly ever-growing electricity demand, emphasising the success of the Belarusian NPP. However, the implementation of this project is not economically viable, given that the current units at the Belarusian NPP are not operating at full capacity.

The Belarusian authorities were also considering the construction of a fourth unit at the Belarusian NPP site or a new nuclear power plant in the Mogilev region. It is possible that Belarus will also see an opportunity to implement these projects.

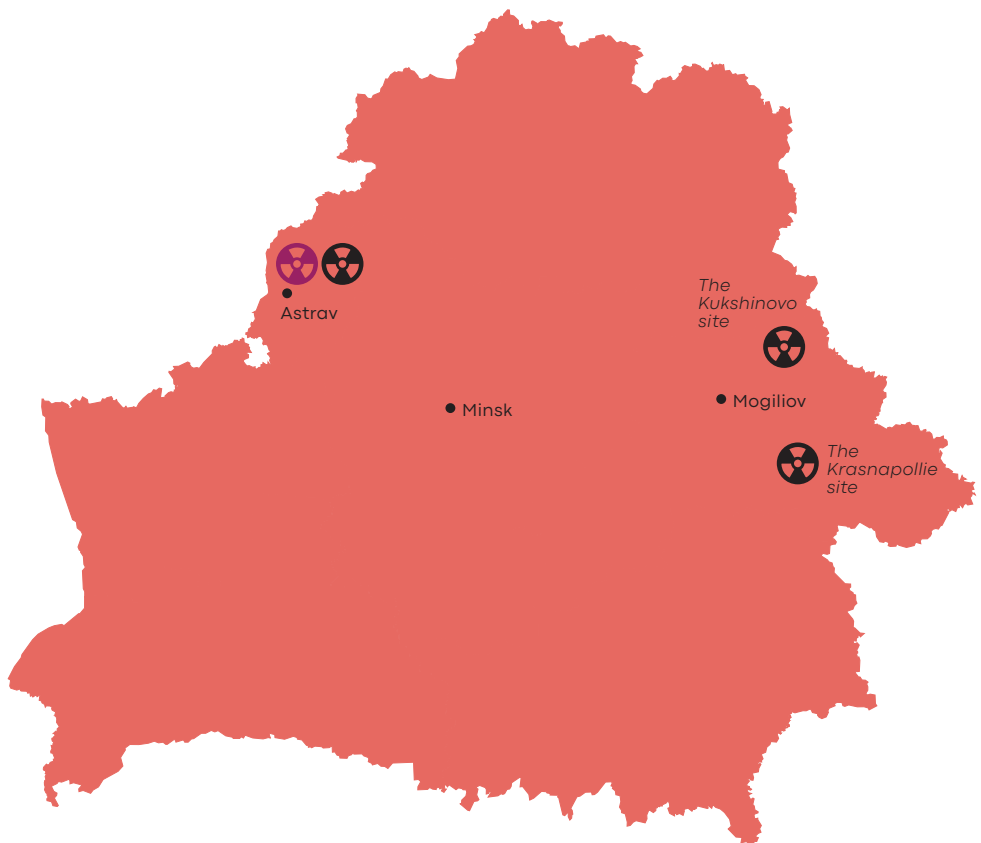
Russia welcomes and supports Belarus's plans to develop nuclear energy, which would be implemented by the Russian corporation Rosatom. These plans would deepen Belarus's energy dependence, which is in line with Russian interests. The Kremlin has expressed support for Belarus's decision to build a third

unit at the Belarusian NPP site and has also urged Minsk not to abandon the plans for building a new nuclear power plant in the Mogilev region. This issue has been a regular topic of discussion at meetings between Rosatom and the Belarusian government.

Despite the plans to develop nuclear energy, the Belarusian authorities are failing to ensure the safe operation of the Belarusian NPP. The plant's operation is frequently interrupted, and its two units are not operating at full capacity due to various technical issues and staff incompetence. According to international practice, nuclear power plant units are usually shut down every 18–24 months for scheduled inspections and maintenance. However, in 2025 alone, one or both units at the Belarusian NPP were shut down at least three times. Shortcomings in Rosatom's technologies, particularly those related to reactor cooling systems, also increase the risk of incidents.

The development of nuclear energy in Belarus will pose a risk to Lithuania's

When announcing the decision to construct a third unit at the Belarusian NPP site in November 2025, Belarusian Deputy Prime Minister Viktor Karankevich also noted that the possibility of building a new nuclear power plant in the Mogilev region was still under consideration.



Operating nuclear power plant



Planned nuclear facilities

national security interests. It is highly likely that Belarus will fail to ensure the safety of the new facilities. The initiation of the new nuclear projects will also distract attention from incidents

at the Belarusian NPP and the technical defects that are causing them. Therefore, the risk of nuclear incidents in Belarus is highly likely to increase.

Entities working against Lithuania's national security interests continue to target strategically important infrastructure and projects, but their methods of operation are changing

Entities with links to Russia, Belarus or China that pose a threat to our national security pursue their interests in strategically important sectors or projects in Lithuania and other Baltic States. Their efforts are not deterred even when their plans are revealed and prevented from proceeding during the investment screening process.

The Lithuanian financial sector, particularly the cryptocurrency segment, remains an attractive target for such entities. Russian citizens seeking to engage in the cryptocurrency sector attempt to conceal their affiliations with Russia, often by using citizenships of a NATO or EU member state.

Companies with links to Russia and Belarus, as well as individual citizens of these countries, have so far been interested in Lithuania's transport and energy sectors. They are also showing an increasing interest in the high-tech sector. They are constantly changing their tactics and looking for new opportunities to gain access to sectors or infrastructure of strategic importance. One method of achieving this is to establish business contacts with entrepreneurs from other European countries or the US, convincing them that the cooperation will yield significant returns, while avoiding direct participation in the initiative. These entities require reliable entrepreneurs from other countries to

conceal their involvement and create a positive image. When their plans fail in Lithuania, they try to implement them in other Baltic States.

Russian entities remain interested in disrupting strategically important projects in Lithuania and other Baltic States. Recently, Russian institutions have been paying a close attention to transport projects implemented by the Baltic States. It is highly likely that these institutions are interested in disrupting the projects in order to limit military mobility in the Baltic States.

Russian intelligence services likely will attempt to collect information about the infrastructure of the Port of Klaipėda and the strategically important cargo handled there by exploiting foreign-registered ship crew members. According

to the intelligence, pro-Russian individuals belonging to crews of ships visiting the port have on several occasions photographed the port infrastructure and sensitive cargo. Russian intelligence services possibly would be willing to use the obtained information to plan sabotage or other kinetic operations.

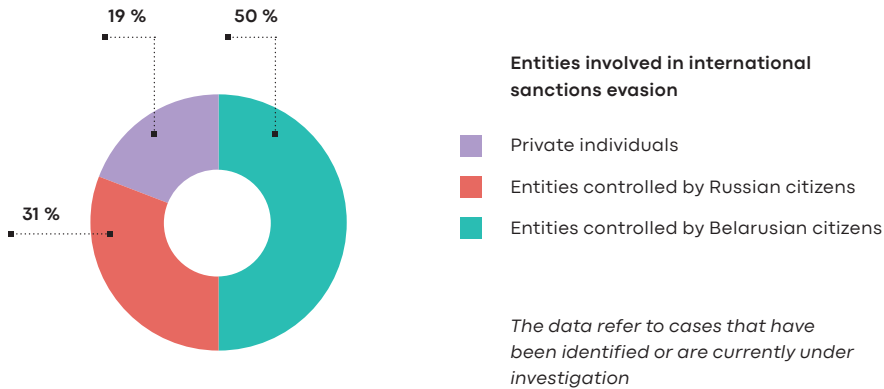
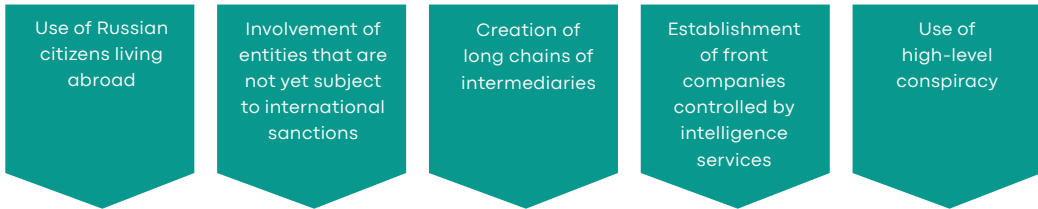
Although the Baltic States have implemented projects aimed at securing their energy independence, Russian entities remain active in pursuing influence within the regional energy sector. They are developing new strategies to resume supplying the Baltic States with Russian energy resources and are looking for individuals who can help them to achieve these goals. While these strategies are unlikely to succeed, the active pursue of these interests likely will continue in the near term.

Although the scale of international sanctions circumvention remains high, the operating models have not changed

Russia and its intermediaries use well-established operating models to evade international sanctions. Russian federal authorities are allocating both

institutional and financial resources to facilitate this, particularly to ensure the supply of equipment and technologies necessary for the military industry.

The most common methods used to evade sanctions



Russian entities are increasingly exploiting companies controlled by Belarusian citizens or Russian citizens who are based in the West and who have the possibility to establish contacts with business entities, high-tech equipment manufacturers, and transport sector representatives operating in Western countries. In certain cases, Russian

citizens seeking to evade sanctions are attempting to revive businesses that have been inactive for some time.

One example of sanctions evasion is the activity of a company called BK Software, overseen by Kirill Lupandin, a Russian citizen. Intelligence suggests that BK Software established business ties

with Asia Pacific Links Limited, a Hong Kong-registered company belonging to Anton Tromifov, a Russian citizen. Asia Pacific Links Limited is subject to EU and US sanctions and is one of the largest suppliers of microelectronic components used in the production of 'Orlan' UAVs to Russian companies. It is almost certain that BK Software deliberately cooperated with Asia Pacific Links Limited, knowing that the end users of the

equipment were Russian entities. Furthermore, it has been established that Lupandin had connections with an FSB unit responsible for infiltrating foreign computer and telecommunications networks. Following the recommendation from Lithuanian intelligence, the presence of Lupandin in Lithuania was declared as a threat to national security due to his activities.



BK Software specialises in computer programming. The company on its website states that it develops and continuously improves innovative information management systems and provides customers with effective telecommunications solutions. It also assists with the integration of satellite and terrestrial equipment and distributes equipment from various foreign manufacturers.

Russian and Belarusian entities seek to operate in the technology sector and use companies established in Lithuania to develop and acquire technologies

Russia and Belarus are seeking to acquire and further develop Western dual-use technologies via companies based in other countries. Their interest in obtaining Western technologies will

remain particularly high, since they are highly unlikely to achieve technological sovereignty in the near term despite their efforts to reduce their dependence on Western technologies.

Western science and research institutions are in the crosshairs of hostile states

Both China and Iran are targeting Western institutions involved in technology research and development. They seek to acquire foreign technological knowledge and technologies themselves for their own benefit: China aims to develop its technology industry, while Iran likely is seeking to continue its nuclear programme. Western countries have been aware of such China's and Iran's activities for some time; it is possible that the two countries will increase their interest in Lithuanian science and research institutions engaged in technology research, as well as the academics working there, in the near to medium term.

China promotes international technological cooperation and engages in scientific espionage, creating financial initiatives that attract foreign scientists and enable acquisition of knowledge and technologies. It actively promotes bilateral agreements with foreign universities to initiate academic student exchange and joint research projects. China invites Western scientists to participate in projects run by the regime, offering them attractive funding prospects, free visits to China, and access to its laboratories and other scientific infrastructure. It is possible that such projects, which Western scientists contribute to, are later used to develop China's civil and military innovation industries.

Iran mainly exploits European scientific institutions to acquire knowledge and technology for its military industry. In recent years, Iranian scientists have obtained European technological research materials that help to develop the country's military industry. This technological knowledge has been obtained through collaboration between Iranian and foreign universities, as well as Iranian nationals conducting technological research at these universities. The Iranian regime also makes use of the material gathered by its students at international conferences and student exchange programmes.

Proposals for scientific cooperation that offer particularly attractive project funding opportunities often only briefly mention the obligations of the scientists involved. The terms of cooperation may pose risks due to links with hostile regimes and their military industries. When receiving an invitation or another request for scientific cooperation from Chinese or Iranian scientific institutions, or from scientists working there, it is important to assess the following:

- Links between the scientific or research institution and the regime
- Potential for the research or product being developed to be used for military purposes
- Sources of funding
- Final products of cooperation and their beneficiaries
- Intellectual property terms and rights
- Other obligations to the inviting institution

RELEVANT TECHNOLOGIES

CHINA



IRAN



Intelligence suggests that entities with links to the Russian and Belarusian military industries have used Lithuanian-based companies NTLab and Kosminis Vytis. The companies operated in the strategically important high-tech sector, while also cooperating with the entities in Russia and Belarus that support their respective military industries.

NTLab and Kosminis Vytis were founded by the Belarusian citizen Dmitry Tcherniakovski, who ran the companies together with his children, Nikolay and daughter Daria. Contrary to their claims, they did not sever their links with Russia and Belarus while developing their activities in Lithuania. They ran companies there and maintained ties with the entities connected to the Russian and Belarusian military industries. Nikolay Tcherniakovski headed the companies Navitron and Sainstech in Russia. The group of companies managed by the Tcherniakovskis also included the Belarusian companies SoftSistemz, Navils, and MikroDizain.

Russian and Belarusian companies that were part of the NTLab group participated in the development of military programmes and cooperated with the entities belonging to the Russian and

Belarusian military industries, such as the Belarusian Military Academy, the scientific-technical centre LEMT, the Skolkovo High Technology Park, the Russian scientific and technical centre Modul, the Russian company Mikron and others. Most of these entities are subject to international sanctions.

NTLab and Kosminis Vytis informed their customers and partners that they were Lithuanian companies with no links to Russia or Belarus. However, this was merely a cover to pursue their interests. The activities and connections of these companies in Russia and Belarus posed a threat to national security interests by enabling Russian and Belarusian military industries to acquire technologies developed in Lithuania and elsewhere, thereby contributing to strengthening of the regimes.

Following an initiative by Lithuanian intelligence in the spring of 2025, the Commission for Coordination of Protection of Objects Critical for National Security assessed the companies' compliance with national security interests. Both companies were found to be incompatible with these interests and were prohibited from continuing their activities in the high-tech sector.

CYBER SECURITY

- **Cyber capabilities of hostile states continue to support their governments' strategic objectives.**
- **The cyberattacks of hostile actors are escalating. The averted cyber sabotage attack against the energy sector of a NATO member state could have left half a million people without heating.**
- **Cyber incidents recorded in 2025 highlighted the vulnerability of the supply chain and the damage cyberattacks cause to critically important processes of organisations crucial to society.**
- **Actors in cyberspace expanded the use of artificial intelligence, in order to increase the scale, speed, and effectiveness of cyberattacks while using fewer resources.**

Intelligence suggests that entities with links to the Russian and Belarusian military industries have used Lithuanian-based companies NTLab and Kosminis Vytis. The companies operated in the strategically important high-tech sector, while also cooperating with the entities in Russia and Belarus that support their respective military industries.

NTLab and Kosminis Vytis were founded by the Belarusian citizen Dmitry Tcherniakovski, who ran the companies together with his children, Nikolay and daughter Daria. Contrary to their claims, they did not sever their links with Russia and Belarus while developing their activities in Lithuania. They ran companies there and maintained ties with the entities connected to the Russian and Belarusian military industries. Nikolay Tcherniakovski headed the companies Navitron and Sainstech in Russia. The group of companies managed by the Tcherniakovskis also included the Belarusian companies SoftSistemz, Navils, and MikroDizain.

Russian and Belarusian companies that were part of the NTLab group participated in the development of military programmes and cooperated with the entities belonging to the Russian and

Belarusian military industries, such as the Belarusian Military Academy, the scientific-technical centre LEMT, the Skolkovo High Technology Park, the Russian scientific and technical centre Modul, the Russian company Mikron and others. Most of these entities are subject to international sanctions.

NTLab and Kosminis Vytis informed their customers and partners that they were Lithuanian companies with no links to Russia or Belarus. However, this was merely a cover to pursue their interests. The activities and connections of these companies in Russia and Belarus posed a threat to national security interests by enabling Russian and Belarusian military industries to acquire technologies developed in Lithuania and elsewhere, thereby contributing to strengthening of the regimes.

Following an initiative by Lithuanian intelligence in the spring of 2025, the Commission for Coordination of Protection of Objects Critical for National Security assessed the companies' compliance with national security interests. Both companies were found to be incompatible with these interests and were prohibited from continuing their activities in the high-tech sector.

CYBER SECURITY

- **Cyber capabilities of hostile states continue to support their governments' strategic objectives.**
- **The cyberattacks of hostile actors are escalating.** The averted cyber sabotage attack against the energy sector of a NATO member state could have left half a million people without heating.
- **Cyber incidents recorded in 2025 highlighted the vulnerability of the supply chain and the damage cyberattacks cause to critically important processes of organisations crucial to society.**
- **Actors in cyberspace expanded the use of artificial intelligence, in order to increase the scale, speed, and effectiveness of cyber-attacks while using fewer resources.**

Cyberattacks are increasing in scale and becoming more destructive

The greatest threat to the information systems of important Lithuanian organisations comes from cyber espionage groups operating on behalf of hostile states. With substantial financial resources, expertise, and motivation to act against organisations in Lithuania and other NATO countries, these groups seek to carry out complex, difficult-to-detect operations designed to obtain sensitive information, to spread disinformation, and since December 2025, carry out destructive attacks against critical infrastructure.

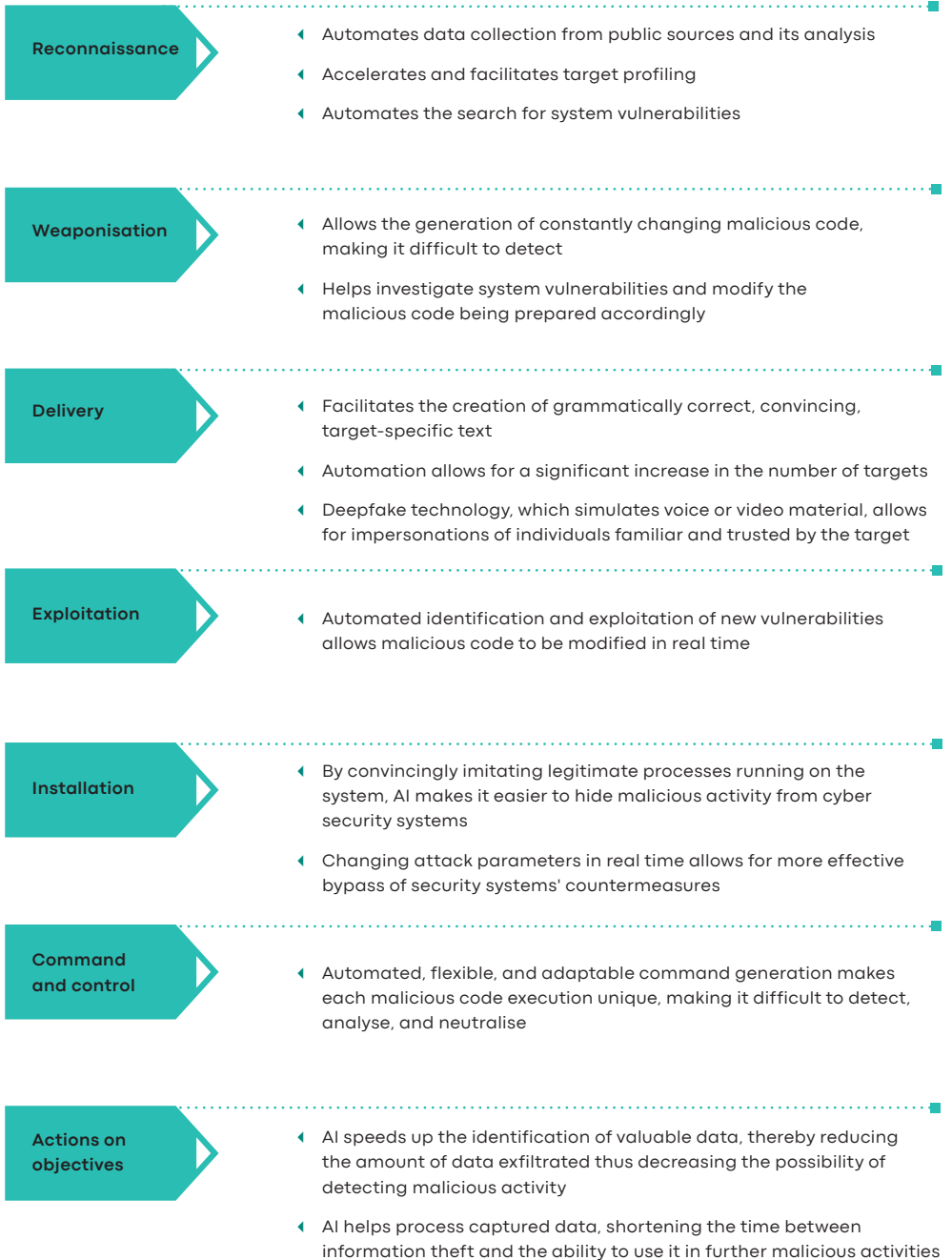
Cyber actors are capable of causing increasing damage to information security, services provided and processes carried out in cyberspace, thus posing a growing threat to national security. In order to avoid the paralyzing effects of cyberattacks, institutions and organisations must strengthen their defensive cyber capabilities and implement alternative measures that would allow them to continue operating without disruption even in the event of a successful cyberattack.

It is almost certain that when a large number of organisations in a single sec-

tor choose the services or products of the same suppliers, the likelihood of successful large-scale cyberattacks increases. Exploiting supply chains creates new vectors of attack. Organisations that pay insufficient attention to cybersecurity may enable hackers to reach other, more resilient organisations in the chain. For example, although the October 2025 outage of Amazon Web Services cloud services was not caused by a cyberattack, it illustrated how a successful cyberattack against a single supplier could affect global supply chains. Services provided by social media platforms Snapchat and Reddit, internet television providers Hulu and Disney+, financial service providers Coinbase and Venmo, and thousands of other organisations were disrupted. The ability to attack one organisation and affect the information systems of all its customers makes supply chain attacks one of the most attractive and effective attack vectors.

Cyber attackers not only continue using proven attack methods but also seek new ways and means to facilitate malicious activities. Improvements in large language models, which the artificial

Practical use of AI at different stages of cyberattacks



intelligence (AI) technologies are based on, enable faster, less resource-intensive, more effective, and more widespread attacks.

Although AI had been used in cyberattacks before, 2025 saw the first documented case of AI being integrated into malicious code. Ukraine's cyber incident response team identified the *LameHug* malicious code used likely by the Russian military intelligence GRU cyber espionage group as a tool to steal information, the commands of which to capture data on the compromised system were generated by AI rather than by hackers themselves. It is very likely that the use of AI has also led to other changes in cyberattacks carried out by hostile states.

For example, AI can be used to effectively collect information on targets' activities, contacts, and communications, which can then be used to prepare malicious emails that do not arouse suspicion. AI also enables hostile states

to use illegally obtained information more quickly and effectively for further malicious activities. This in turn allows adversarial states to prepare in advance for political decisions that are unfavourable to them, to conduct discrediting and disinformation campaigns in real time, and, in the event of war, to effectively identify and eliminate targets.

It is almost certain that geopolitical tensions, the development of cyber capabilities by hostile states and the criminal world, as well as new technologies, will increase the threat level in the cyberspace of Lithuania and other NATO countries in both the short and long term. Continuous updates and practical applications of critically important Lithuanian organisations' cyber security policies, considering the innovations in cyber threat landscape and changes of organisations' IT processes and infrastructure, reduce risks not only to the organisation itself, but also to entities related to it, as well as to Lithuania's national security.

Examples of cyberattacks in 2025 that disrupted the processes of organisations critical to society:

- In January, an attack on Slovakia's national land registry, described by Slovak Minister of Agriculture as the largest cyberattack in the country's history, disrupted activities of state and private entities that depend on these data.
- In September, an attack on Collins Aerospace's MUSE software, used to manage passenger check-in and boarding, disrupted operations at Heathrow, Brussels, Berlin, and Dublin airports, resulting in flight delays and cancellations.
- In December, a coordinated large-scale attack against electricity and heat supply organisations was prevented in Poland. Polish Prime Minister Donald Tusk indicated that there were many reasons to believe that the attack had been carried out by groups directly linked to Russian services. It has been reported that if the attack had been successful, half a million Polish citizens would have been left without heating during the winter. Poland's Minister of Digital Affairs stated that the attack came very close to disrupting the electricity supply.

INFLUENCE ACTIVITIES AGAINST LITHUANIA

■ **Lithuanian nationals who support the Russian regime help to implement hostile Russian and Belarusian information policies against Lithuania.** They collaborate with employees from Belarusian and Russian propaganda outlets, grant them interviews, and participate in anti-Lithuanian propaganda campaigns.

■ **Russian Presidential Administration shapes propaganda narratives accusing the Baltic States of systematically distorting the history of World War II, glorifying Nazi collaborators, and persecuting Russian speakers.** The Russian Ministry of Foreign Affairs plays a key role in disseminating accusations of Russophobia within international institutions. Russia is exploiting these accusations in an attempt to exert pressure on Lithuania and other Baltic States and likely to justify its aggressive foreign policy and geopolitical interests.

■ **The Moscow Patriarchate exerts significant influence over its subordinate dioceses abroad, including the Orthodox Diocese of Vilnius and Lithuania, which enables Russia to extend its reach within the Lithuanian Orthodox community.** Although the diocese's leadership has officially expressed a strive for partial self-government status, this status does not permit independent decision-making and is motivated by an effort to avoid public criticism of its subordination to the Moscow Patriarchate.

Pro-Russian individuals contribute to the implementation of hostile states' goals in Lithuania

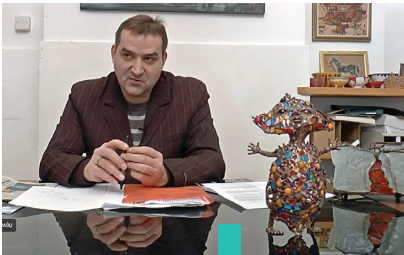
Lithuanian nationals who support the Russian regime and its aggressive policies assist in the implementation of hostile Belarusian and Russian information and history policies towards Lithuania. They collaborate with employees from Belarusian and Russian propaganda outlets, grant them interviews, and participate in anti-Lithuanian propaganda campaigns. In interviews with Russian or Belarusian propaganda outlets, these pro-Russian individuals portray Lithuania as an undemocratic state under Western control, with a Nazi and Russophobic regime in power. They claim that elections are undemocratic and illegitimate, that freedom of speech is restricted, and that Lithuanian citizens are persecuted based on their nationality and political views. They also accuse Lithuania of interfering in Belarus's internal affairs and inciting war with Russia, while advocating cooperation with these countries' autocratic regimes. By taking these actions, pro-Russian individuals are

helping the Belarusian and Russian regimes to spread propaganda against Lithuania.

The activities of pro-Russian individuals that violate Lithuanian law are prevented by legal means. Consequently, some pro-Russian individuals who wish to avoid legal responsibility flee to Belarus or Russia, where they actively engage in activities directed against Lithuania. They actively cooperate with the Russian and Belarusian regimes, implement their information and history policy objectives to undermine Lithuanian statehood, and express support for the activities of pro-Russian groups operating in Lithuania. Those who fled to Russia or Belarus face financial difficulties and a lack of social connections. They only interact with a small group of fellow pro-Russian individuals who have also fled the Baltic States and are forced to carry out constant instructions from Russian and Belarusian entities in exchange for a small reward.

Edikas Jagelavičius, a Lithuanian national hiding from Lithuanian law enforcement in Belarus, presents the programme 'Neighbours' on the Belarusian regime-controlled radio station 'Belarus', which regularly broadcasts anti-Lithuanian propaganda. Jagelavičius is wanted for assisting another state in carrying out hostile activities. He has also been charged with forging documents when setting up a pro-Russian association in Lithuania, which organised trips to Belarus and Russia and carried out activities favourable to these countries.

Giedrius Grabauskas, one of the authors of the Russian propaganda book 'The History of Lithuania', is hiding from Lithuanian law enforcement in Russia. The book promotes a narrative that undermines Lithuanian statehood in line with Russia's history policy objectives. Grabauskas is currently facing criminal charges in Lithuania for defaming the Lithuanian anti-Soviet resistance movement.



Giedrius Grabauskas and Edikas Jagelavičius
A frame from a Youtube video

The tendency of pro-Russian activists to flee to Belarus or Russia has been observed in all the Baltic States. This intensified after Russia's full-scale invasion of Ukraine in 2022, when pro-Russian activities began to face stricter restrictions. The movement 'Baltic Community "Together"' (Pribaltiyiskoye Zemlyachestvo 'Vmeste') was established in Russia to unite pro-Russian activists who had fled the Baltic States to Russia. Jagelavičius and Grabauskas also participate in meetings of this movement.

The Foundation for the Support and Protection of the Rights of Compatriots Living Abroad, which is subject to EU sanctions, finances the legal defence of pro-Russian public figures in Lithuania and their initiatives within international organisations that are directed against Lithuania and in Russia's favour. By doing so, Russia is attempting to support the activities of pro-Russian groups in Lithuania and discredit the country in the eyes of the international community.

Russia is stepping up its information campaigns on social networks, using constant propaganda narratives to support them

Although international sanctions and national restrictions have reduced Russia's ability to disseminate propaganda in Lithuania, it has not abandoned the goal to influence Lithuania's information space. Russian propaganda narratives directed against Lithuania remain unchanged, but they are increasingly being disseminated in disguised forms. The aim is to create the impression that pro-Russian messages originate from within Lithuanian society. In the Lithuanian context, social networks have become primary means for Russia to

disseminate propaganda. They allow Russia to circumvent restrictions applied to propaganda channels, facilitating the implementation of targeted operations and long-term campaigns aimed at instilling distrust in state institutions, fomenting discord, eroding confidence in NATO, and discrediting support for Ukraine. Social media algorithms enable rapid spread of information, and Russian propaganda channels often exploit the credibility of independent news sites or influencers by impersonating them.

We assess that Russia is adapting to the changes in how information is consumed and is actively using TikTok to disseminate its narratives to a broader audience. Russian propaganda on TikTok comes in the form of entertaining videos, memes, and audio tracks that conceal a message serving Russia's interests. The aim is to engage young people and influence their opinions on significant political and social issues, as well as to erode their trust in traditional news sources. TikTok frequently employs narratives that seek to discredit Lithuanian history, undermine national identity, and cast doubts on the future of the state. Since 2022, Russia has repeatedly accused the Baltic States of systematically distorting the history of World War II, glorifying Nazi collaborators, persecuting Russian speakers on ethnic and political grounds, and destroying Russian culture. These and other long-standing narratives in Russian propaganda that discredit Lithuania have been shaped by the Russian Presidential Administration. This institution occupies a central place in the Russian propaganda hierarchy and is the most important in the Kremlin regime.

The Russian Ministry of Foreign Affairs plays a key role in disseminating accusations of Russophobia within international

institutions. Through public statements and diplomatic channels, the ministry seeks to highlight the alleged Russophobic policies of the Baltic States. Every year, the Russian Foreign Ministry prepares reports on the human rights situation in other countries. In these reports, the Baltic States are labelled the most Russophobic, with Lithuania accused of violating the rights of Russian speakers, persecuting dissidents, and falsifying history on a systemic level.

These accusations are supported by front organisations established to spread Russian influence, such as academic institutions, foundations, and analytical centres that conduct pseudoscientific research in line with the Kremlin's narrative. Their task is to demonstrate that the Baltic States support Nazi ideology and pursue Russophobic policies. Such organisations include the Immanuel Kant Baltic Federal University; the Foundation for the Support and Protection of the Rights of Compatriots Living Abroad, established by the Russian Ministry of Foreign Affairs and its subordinate federal agency Rossotrudnichestvo; and the Historical Memory Fund (established at the initiative of the Russian Presidential Administration). These organisations hold conferences, exhibitions and other events dedicated to the Baltic States

Repetition is one of the defining features of Russian propaganda. Information campaigns are based on a few recurring narratives that act as standard models, and then are adapted to specific situations by Russian propaganda outlets. This was evident in Russia's propaganda campaign targeting the disconnection of Lithuania and other Baltic States from the BRELL electricity system. In implementing this campaign, Russia employed four propaganda narratives. Propaganda channels and social networks were used to disseminate information targeting the Baltic States, while automated social media accounts spread AI-generated images disparaging the decision to disconnect from BRELL, thereby increasing the reach of information.

1 The Soviet era brought more benefits than harm to Lithuania.

Russian propaganda portrayed the BRELL system, which was created during the Soviet era, as a reliable and effective infrastructure that ensured low electricity prices. Leaving the system was presented as an ill-advised decision that would jeopardise the long-term benefits of previous energy integration.

2 Lithuania is not a sovereign state; it merely follows the instructions from the EU and the US.

Russian propaganda claimed that Lithuania had no independent energy strategy and was instead blindly following the instructions of more powerful allies that did not serve its interests. This narrative aimed to undermine Lithuania's independence by suggesting that its strategic decisions were influenced by external forces.

3 Lithuania is pursuing a provocative policy towards Russia.

Lithuania's withdrawal from BRELL was presented as another provocative move against Russia, exacerbating tensions in the region and undermining energy security. Russian officials repeatedly claimed that Lithuania was deliberately provoking Russia, disregarding the negative consequences for its energy sector and economy. Leaving the BRELL system was presented as further evidence of Lithuania's Russophobic policy.

4 Hostility towards Russia is damaging Lithuania's economy.

Russian propaganda portrayed the withdrawal from BRELL as an economically damaging move that would lead to higher electricity prices, lower energy security and hinder Lithuania's long-term economic development. It was argued that Lithuania should prioritise pragmatic economic relations with Russia over political ambitions.



in Russia. Pro-Russian figures from Lithuania are often invited to speak at these events, where Russia's fabricated accusations are presented as expert assessments. We assess that Russia is exploiting these accusations in an attempt to exert pressure on Lithua-

nia and other Baltic States within international organisations. By repeatedly accusing the Baltic States of violating the rights of Russian speakers and glorifying Nazism, Russia is likely seeking to justify its aggressive foreign policy and geopolitical interests.

Despite declaring a strive for greater independence, the Orthodox Diocese of Vilnius and Lithuania remains dependent on the Moscow Patriarchate

The Orthodox Church plays a significant role in shaping and supporting ideological narratives of the Russian regime. Russia employs the Orthodox Church to spread the idea of the 'Russian world' and strengthen its influence in foreign countries, particularly those with sizeable Orthodox and Russian-speaking populations. Due to its strictly hierarchical structure, the Moscow Patriarchate exerts significant influence over its subordinate dioceses abroad. Subordination of the Orthodox Diocese of Vilnius and Lithuania to the Patriarchate enables Russia to extend its reach within the Lithuanian Orthodox community.

The support of Patriarch Kirill of Moscow for Russia's war against Ukraine prompted some clergymen of the Orthodox Diocese of Vilnius and Lithuania to express their negative stance on the aggression. In response to pressure from public and the faithful, the diocese's leadership publicly condemned the war and repeatedly announced its strive for greater independence from the Moscow Patriarchate. However, no significant changes have occurred in this regard so far.

The diocese's leadership has officially expressed its strive for independence and requested the Moscow Patriarchate to grant it partial self-government status. Contrary to the claims of the diocese's representatives, this status is neither exclusive nor close to autonomy, and it does not permit independent decision-making. Even if the diocese had been granted this status, the Patriarchate would still have significant influence over the most important management decisions, including the appointment of church leaders, the formation of management bodies, and the approval of court decisions. All Patriarchate decisions would also continue to apply to the diocese. We assess that the Diocese of Vilnius and Lithuania is seeking partial self-government in order to avoid public criticism of its subordination to the Moscow Patriarchate while still remaining entirely under its influence.

The subordination of the Diocese of Vilnius and Lithuania was discussed at a meeting of the Holy Synod of the Moscow Patriarchate. However, until now the Patriarchate has not granted greater autonomy to the diocese. On the contrary, in response to the diocese's

public statements about its strive for greater independence, the leadership of the Patriarchate has established a division charged with maintaining control of overseas dioceses subordinate to the patriarchate.

The leadership of the Diocese of Vilnius and Lithuania has so far sought to project an image of independence. They have avoided emphasising their subordination to the Moscow Patriarchate and refrained from publicly expressing support for Russia. The establishment of a new Orthodox church structure, the Exarchate of the Patriarchate of Constantinople in Lithuania, has consolidated the clergy of the Diocese of Vilnius and Lithuania, encouraging them to play a more active role in retaining and attracting new members to their community. The leadership of the Moscow Patriarchate is monitoring the expansion of the church subordinate to the Patriarchate of Constantinople in Lithuania. We assess that the Moscow Patriarchate views this development as a threat to its interests and will therefore attempt to limit the activities of the newly established church and maintain its influence over the Diocese of Vilnius and Lithuania.

EXTREMISM AND TERRORISM

- **Several attempts to establish nihilistic right-wing extremist groups have been identified in Lithuania in recent years.** Followers of this ideology are often young and vulnerable individuals whose involvement often begins with visiting right-wing extremist channels on social media. New group members are encouraged to commit criminal offences, including murder. The growing popularity of nihilistic right-wing extremism is increasing the likelihood of 'lone wolf' attacks.
- **It remains possible that Russian and Belarusian intelligence services will use right-wing extremists living in Western countries to carry out acts of sabotage in the near term.** Belarusian and Russian intelligence services and right-wing extremists operating in Western countries share some objectives. They both seek to cause panic in Western societies and undermine trust in government institutions and the democratic system by performing high-profile criminal acts.
- **Islamist terrorist organisations and their followers are targeting minors.** The number of young people involved in planning, supporting or carrying out attacks is increasing in Europe. These organisations and their supporters use new technologies, such as artificial intelligence, to create violent content that appeals to minors and encourages their radicalisation. There have been isolated cases of minors in Lithuania expressing an interest in Islamist propaganda.

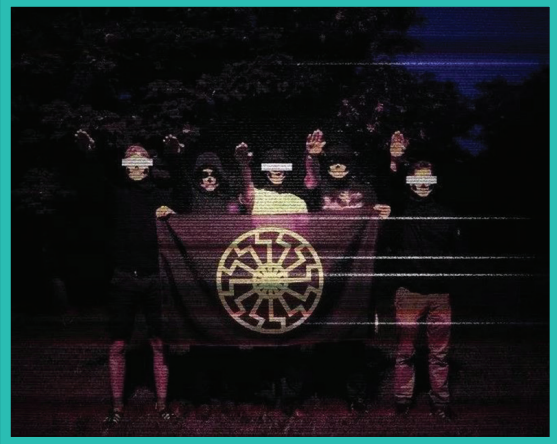
The rise in popularity of nihilistic right-wing extremism among psychologically vulnerable minors is increasing the likelihood of 'lone wolf' attacks

Several groups promoting right-wing extremist ideology are currently operating in Lithuania. These groups are driven by a shared animosity towards foreigners. Some groups combine radical chauvinism with martial arts, using violence to achieve their ideological objectives. There are also several accelerationists in Lithuania, who seek to hasten the allegedly inevitable race war by using violence. Followers of this ideology often carry out attacks using 'lone wolf' tactics.

Several attempts to establish nihilistic right-wing extremist groups have been identified in Lithuania in recent years. Compared to other right-wing extremist movements, this ideology poses a greater threat due to several

of its defining features. Supporters of nihilistic right-wing extremism do not consider any form of violence (physical, psychological, or sexual) to be a means to an end, rather an end in itself. They also combine ideological tenets of right-wing extremism with Satanism and occultism, rejecting any moral standards as a sign of weakness.

Followers of nihilistic right-wing extremism are often very young and vulnerable individuals, typically aged 13–14 (and sometimes even 10–11). Many of them suffer from mental health issues and find it difficult to form relationships with their peers in real life. Instead, they spend almost all their social time on social networks.



The Maniac Murder Cult, often referred to on social networks by the acronym MKY or MKU, based on its Russian name, 'Manyaki: Kult Ubistva', is the most popular international nihilistic right-wing extremist network among young extremists living in Lithuania. Formed in Russian-speaking Eastern European countries towards the end of the previous decade, it later spread to other regions of Europe and North America. Individuals identifying with MKY have committed or planned to commit murders in some European countries. All nihilistic right-wing extremist groups that have attempted to establish themselves in Lithuania have been influenced by the MKY's ideological principles.

Involvement in nihilistic right-wing extremist groups often starts with visiting right-wing extremist channels on TikTok or playing popular online games such as Roblox and World of Tanks. Later, radicalised individuals continue to communicate on platforms such as Telegram and Discord. Their involvement in criminal activities occurs in several stages. First, new group members are encouraged to commit minor offences,

such as graffiti vandalism or smashing windows. They are then persuaded to commit acts of violence against representatives of racial, religious and ethnic minorities, or homeless people. They are also encouraged to exert psychological pressure on psychologically vulnerable individuals on social networks, forcing them to harm themselves or commit suicide. Finally, members of the nihilistic right-wing extremist network are encouraged to commit murder and record it on video.

Parents, teachers and others close to adolescents often fail to notice when they first become involved in extremist activities. Right-wing extremist ideology on social media is often disguised and presented as dark humour, memes, or works of fiction. Even when parents notice their children's interest in right-wing extremist ideologies, they often fail to recognise the associated threats and do not take action to stop the radicalisation process.

The following signs may indicate a young person's involvement in a right-wing extremist group on social media:

Social isolation

-
Spending most of their time communicating on social networks
-
Use of terminology, symbols and images that are typically associated with a specific social group
-
Spreading extremist ideological views and conspiracy theories during interactions with individuals in the immediate circle
-
Purchasing items bearing right-wing extremist symbols
-
Interest in the manufacture of makeshift weapons and explosives

Intelligence services of hostile states view right-wing extremists as potential perpetrators of their operations

The GRU has attempted to recruit right-wing extremists living in European countries to carry out its operations. Yuri Sizov, an employee of the branch of the GRU responsible for organising sabotage operations in Western countries, visited Russian-speaking right-wing extremist channels on Telegram. Pretending to be a right-wing extremist, he used one of his Telegram accounts to try to find people with contacts to right-wing extremists living in EU countries. While communicating on these channels, Sizov used hateful rhetoric and incited the killing of Black people and immigrants.

Islamist terrorist organisations and their followers are targeting minors

An increasing number of young people in Europe, including minors, are involved in planning, supporting or carrying out Islamist terrorist attacks, or spreading terrorist propaganda.

Islamist terrorist organisations and their supporters use new technologies, such as artificial intelligence, to create violent content that appeals to minors. Islamic State propaganda is designed to appeal to young people and is shared on popular social networks such as TikTok and gaming platforms like Roblox. Those who show an initial interest are later invited to closed chat groups on social networks such as Telegram. There, they

become radicalised and begin to plan attacks, to identify targets, and look for ways to acquire weapons.

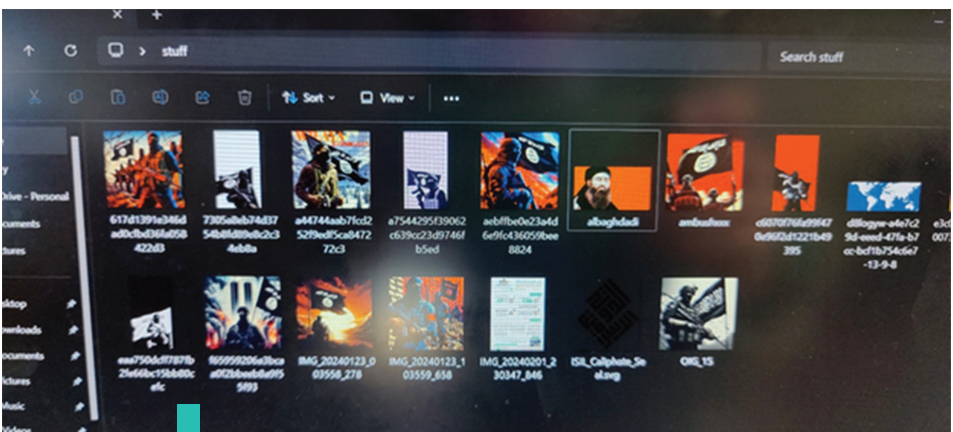
Young people radicalised by Islamist ideology most often target civilians, officials, Christian places of worship, and the LGBT+ community. The conflict between Israel and Hamas has intensified Islamist propaganda, fuelling hostility towards members of the Jewish community among some radicalised young people in Europe. Islamist propaganda glorifies attacks against those who desecrate the Qur'an, presenting them as role models for young people.

In 2025, Belarusian or Russian intelligence services highly likely attempted to recruit right-wing extremists living in Lithuania via social networks, with an aim of involving them in covert operations against Lithuania. Right-wing extremists were offered financial rewards in exchange for attacking members of the Belarusian community and gathering intelligence.

Belarusian and Russian intelligence services and right-wing extremists operating in Western countries have some shared objectives. Both seek to cause panic in Western societies and undermine their trust in government institutions and the democratic system by organising high-profile criminal acts. Therefore, it remains possible that Russian and Belarusian intelligence services will use right-wing extremists living in Western countries to carry out acts of sabotage in the near term.

In the near term, terrorist propaganda disseminated via social networks and gaming platforms almost certainly will encourage minors to become involved in terrorist activities in Europe. This will be exacerbated by social integration problems among minors, their traumatic personal experiences, and a lack

of parental control. Although terrorist organisations will primarily seek to recruit adults capable of carrying out large-scale attacks, they likely will target children and young people to carry out simpler attacks and provide logistical and financial support.



Islamic State propaganda material viewed by a minor in Lithuania. There have been isolated cases of minors in Lithuania showing interest in Islamist propaganda. Europe has seen an increase in the number of minors arrested for Islamist terrorist crimes.

Terrorist attacks in Europe, 2025



The threat of terrorism in Europe will remain high

The threat of Islamist terrorism in Europe remains high. While most terrorists have no links to the Islamic State, they have been radicalised by its propaganda online. The Islamic State of Khorasan Province, the Islamic State's branch in Afghanistan, is recruiting followers within Central Asian diaspora communities, posing a security risk to Europe.

As immigration from Central Asia to Lithuania has increased, individuals with radical views or links to terrorism have been identified within the Central Asian community. Given the availability of Islamist propaganda online, terrorist attacks carried out by radicalised individuals are possible in Lithuania.

While it is unlikely that Lithuania will become a target for Islamist terrorists in the near term, attempts by radicalised individuals residing in Lithuania to spread propaganda, establish support groups for extremist ideologies, and finance terrorist organisations are possible.

Threats to the security of the state come from various sources – hostile countries, individual actors, various technologies, and phenomena. In recent years, hostile countries have actively used electronic warfare capabilities and unmanned aerial vehicles – these are symbolically depicted on the cover, which was created using an artificial intelligence tool.

Author and Editor: Defence Intelligence and Security Service under the Ministry of National Defence and State Security Department of the Republic of Lithuania

06.02.2026. Circulation: 1,050 units. Order GL-28

Layout by the Publishing Section of the General Affairs Department of the Ministry of National Defence, Totorių str. 25, LT-01121 Vilnius.

Printed by the Military Cartography Centre of the Lithuanian Armed Forces, Mūitinės str., Domeikava, LT-54359 Kaunas District.

www.kam.lt

ISSN 2669-2732

© Ministry of National Defence of the Republic of Lithuania, 2026

© State Security Department of the Republic of Lithuania, 2026



The Defence Intelligence and Security Service (AOTD) is an intelligence agency under the authority of the Minister of National Defence. AOTD is responsible for conducting intelligence and counter-intelligence activities in the defence, military-political, military-economic, military-technological, and military-information areas. It is also responsible for information security within the National Defence System in Lithuania and abroad.



The State Security Department (VSD) is an intelligence agency accountable to the Parliament and the President of the Republic of Lithuania. VSD is responsible for conducting intelligence and counter-intelligence in the social, political, economic, scientific, technological, and informational fields. It ensures the security of the diplomatic service and of other institutions of the Republic of Lithuania abroad as well as the protection of classified information.