STATE
SECURITY
DEPARTMENT
OF THE REPUBLIC
OF LITHUANIA

DEFENCE
INTELLIGENCE AND
SECURITY SERVICE
UNDER THE MINISTRY
OF NATIONAL DEFENCE

KAM
ANTRASIS DEPARTAMENTAS

2025

NATIONAL THREAT ASSESSMENT

2022

Russia starts a full-scale invasion of Ukraine

Lithuania ends imports of Russian gas

Russia threatens to retaliate against Lithuania for restricting the transit of sanctioned goods to and from the Kaliningrad Region

ChatGPT greets the world

2021

Unit 1 of the Belarusian nuclear power plant becomes operational

Illegal migration crisis orchestrated by the Belarusian regime starts

The Taliban takeover in Afghanistan

China begins coercion against Lithuania after opening of the Taiwanese Representative Office in Vilnius

2023

Putin and Lukashenka announce the deployment of nuclear weapons in Belarus

Russia starts a sabotage campaign in Europe

Wagner Group mutiny ends in failure

Hamas terror attack against Israel

2024

The Baltic States officially notify their withdrawal from Russian-controlled electricity grid

Lithuania and Germany sign defence cooperation agreement

A series of incidents, one of which caused by a ship attributed to Russia's shadow fleet, results in damage to underwater infrastructure in the Baltic Sea

STATE SECURITY
DEPARTMENT OF
THE REPUBLIC OF
LITHUANIA

DEFENCE
INTELLIGENCE AND
SECURITY SERVICE
UNDER THE MINISTRY
OF NATIONAL DEFENCE
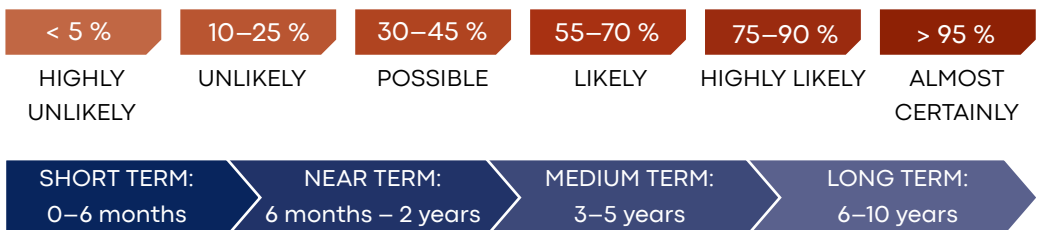
2025

NATIONAL THREAT ASSESSMENT

CONTENTS

INTRODUCTION

The National Threat Assessment by the State Security Department of the Republic of Lithuania (VSD) and the Defence Intelligence and Security Service under the Ministry of National Defence of the Republic of Lithuania (AOTD) is presented to the public 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 consolidated, 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 14 February 2025.

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

< 5 %	10–25 %	30–45 %	55–70 %	75–90 %	> 95 %
HIGHLY UNLIKELY	UNLIKELY	POSSIBLE	LIKELY	HIGHLY LIKELY	ALMOST CERTAINLY

SHORT TERM: 0–6 months	NEAR TERM: 6 months – 2 years	MEDIUM TERM: 3–5 years	LONG TERM: 6–10 years

Darius JAUNIŠKIS

Director of the State Security Department of the Republic of Lithuania

Colonel Elegijus PAULAVIČIUS

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

FOREWORD

The Lithuanian intelligence community presents the tenth iteration of the National Threat Assessment. The scope and form of this document has changed over the years, but the main sources of threats to Lithuania remain the same: an increasingly aggressive Russia, Belarus with its progressing dependence on Russia, and in recent years, an increasingly hostile China.

The last decade has been marked by mounting tension. Russia's aggressive rhetoric has turned into a war against Ukraine marked by crimes against humanity and sabotage against the West. The Belarusian regime, which has brutally suppressed its people's desire for freedom and justice, has orchestrated an unprecedented illegal migration crisis against Lithuania, Poland, and Latvia. China has become one of the main supporters of Russia's aggression.

Unfortunately, the situation is unlikely to improve in the near term. Despite huge losses in Ukraine, the heavy burden on its economy, and impoverishment of its own society, Russia continues to intensify its war effort and resorts to nuclear blackmail against the West. Following the Kremlin's lead, other autocracies hope to disrupt the existing world order and create a new one, based on coercion and dehumanisation, not on respect for human rights and the sovereignty of states.

We know it, we are preparing for it, we trust in resilience and awareness of our citizens, and we believe in the superiority of our free world over dictatorships.

Russia constantly tries to rebuild its spy network in Lithuania and allied countries, which was disrupted in retaliation for Russia's invasion of Ukraine; the Belarusian KGB is aggressively trying to recruit people who cross the Belarusian border; and China is actively engaged in cyber espionage and remote recruitment. All of this requires constant and full counterintelligence attention.

We are also witnessing increasingly aggressive and dangerous forms of malicious activity that we have not seen since the Cold War – in 2024, there were dozens of sabotage operations targeting infrastructure, energy, transport, information systems, and objects of historical memory in Lithuania and other European countries supporting Ukraine. We assess that these attacks are usually organised by Russian intelligence services and carried out by individuals recruited on social networks, sometimes without even knowing who they are working for.

The world has entered the age of artificial intelligence. Not only friendly countries are investing in the development of quantum computers, sensors, and

new cryptography. If we do not allocate adequate intellectual and financial resources to mastering the latest technologies, we would not only risk falling behind our rivals but also risk losing touch with our partners and allies.

To mark the tenth iteration of the National Threat Assessment, its cover features some of the major events that have influenced the security situation in the region and the world: not only the threats we faced, but also the actions we – Lithuania and our allies – took for the sake of our security. It is particularly important today to underline that Lithuania has secured its energy independence, and the 2024 elections confirmed that Lithuanian society is resistant to Russian attempts to exert greater influence.

Our intelligence community will continue to dedicate their operational, analytical, and organisational capabilities to ensure that threats to the Lithuanian state and society, as well as to those of our allies, are prevented and any damage is mitigated. We are doing this by increasingly cooperating with our partners. We hope that this document will contribute to strengthening the understanding of threats we face and therefore, the resilience, as knowledge is a powerful weapon.

SUMMARY

■ **Russia's ruling regime highly likely considers relations with the West to be in the grey zone between war and peace.** It resorts not only to diplomatic pressure but also employs violent actions against countries that do not align with Russia's interests. Russia almost certainly is trying to influence Western societies, increase distrust in state institutions, and force political leaders to weaken support for Ukraine.

■ **A diplomatic solution to the war in Ukraine is unlikely in the short term.** The Kremlin's perceived superiority over Ukraine-supporting Western democracies almost certainly will drive its war efforts until it secures substantial concessions. International pressure has no effect on Russia's position, and its strengthening alliances with Iran and North Korea indicate that in its confrontation with the West, Russia is willing to collaborate with any ally or use every possible means.

■ **Russia has the resources to continue the war.** The conflict forces Russian leadership to allocate significant financial resources for the war effort, but Russia will not only be able to maintain a similar level of war funding in the near term but is likely to further increase it. Current military spending has a negative effect on Russia's economy, but it has no impact on the Kremlin's foreign and security policy. The Putin regime considers itself to be in full control of domestic situation, and threats to its stability are unlikely in the short term.

- **Russia continues to strengthen its military capabilities.** Despite the losses suffered in the war in Ukraine, Russia continues to increase its military personnel, devote significant attention and resources to the development of its military industry, and pursue its ambitious military reform.

- **The military grouping in the Kaliningrad Region remains capable of performing essential tasks.** Russia is transferring ground troops and combat equipment to Ukraine even from the regions closest to NATO, including the Kaliningrad Region. However, although the involvement of Kaliningrad's naval and air components in the military action is weaker, they would be sufficient to disrupt NATO's actions in the Baltic Sea region in the event of a conflict.

- **After staging another rigged presidential election, Lukashenka has consolidated his power.** In the near term he will seek to be recognised by the West as legitimate head of the state. Belarus is providing increasing support for the Kremlin's international policy initiatives; it will remain Russia's closest ally and will not change its strategic decision.

- **Belarusian intelligence services act against Lithuanian citizens visiting Belarus in a manner which is incompatible with international law.** Lithuanian citizens are illegally detained and prosecuted for their political views and criticism of the Belarusian regime. These regime's actions are stimulated by the intension to exert pressure on Lithuania for it to reconsider its policy towards Belarus, and to reinforce the narrative of Belarus surrounded by hostile countries.

■ **China is helping Russia to continue its war against Ukraine.** Beijing's support is driven by the belief that the Putin regime should not lose the war and the assessment that the war aligns with China's interests as it presents a challenge to the West by draining its resources. Strengthening economic, energy, and military cooperation between China and Russia will not only result in Kremlin's significantly increased ability to continue the war but will deepen Russia's dependency on China.

■ **Russia is stepping up its involvement in Africa.** Using its proven low-cost, high-impact strategy of exploiting instability and propping up military regimes as well as actively spreading disinformation and propaganda against the West, Moscow seeks to strengthen its position in the continent, gain allies, and reduce its international isolation.

■ **International terrorist organisations are exploiting the conflict in the Middle East.** They spread anti-Western and anti-Semitic narratives, seek to exacerbate social polarisation, and encourage Muslims living in the West to engage in Jihad. Terrorist trends in other European countries have an impact on terrorism-related threats in Lithuania, as Islamist online propaganda poses a risk that easily radicalised individuals in Lithuania may adopt extremist views.

Ministry of National Defence of Lithuania

RUSSIA

■ By conducting sabotage operations Russia is trying to influence Western societies, increase distrust in state institutions, and force the West to weaken support for Ukraine.

■ Threats to the stability of the Kremlin regime are unlikely in the short term. Putin's perceived superiority over Western democracies will drive his resolution to wage war until he secures substantial concessions.

■ Russia has enough economic resources to finance the war against Ukraine in the near term and likely would be capable to step up its defence spending if such a need should arise. However, this trend will increase the risk to the long-term economic stability of the country.

■ The growth of Russia's military power is directly linked to the course of the war in Ukraine. The reduced demand on the front line would allow Russia to accelerate the formation of new troops and increase its reserves of arms and ammunition.

■ Revision of the nuclear doctrine was a message oriented towards the West. Russia sought to strengthen the deterrence and coerce Western states to reduce military support for Ukraine or cease it altogether.

Russian intelligence services conduct sabotage activities to undermine Western support for Ukraine

The methods employed by Soviet-era intelligence services, including sabotage and political assassinations, are still in use by their successors, Russian intelligence services. For almost two decades, Russia has been carrying out assassinations against regime critics at home and abroad. However, the sabotage campaign that began in 2023 and escalated in 2024 shows Kremlin's firm resolve to act not only against its critics but against the entire West. Sabotage activities against Lithuania commenced with the defacement of monuments of historical importance and gradually evolved into more resource-intensive operations in 2024.

We assess the Russian regime highly likely considers relations with the West to be in the grey zone between war and peace. It resorts not only to the usual foreign policy instruments, such as diplomatic pressure, but also employs a range of measures that are not typically associated with peacetime, including violent, covert actions, against states that do not align with Russia's interests. Russian intelligence services empowered by the country's political elite carry out sabotage operations similar to those during wartime, with the aim of causing harm to the West without entering into an open conflict. Russia's sabotage operations transcend national borders: they are systematically and concurrently executed in multiple countries. This sabotage campaign is an integral part of Russia's aggressive policy towards the West, rather than isolated incidents against individual states.

Russian intelligence services are using a multi-tiered system of intermediaries to conceal the real initiators and coordinators of sabotage operations. Individuals recruited for these actions by Russian intelligence services on social networks, particularly *Telegram*, fit the profile of people interested in quick and easy financial rewards. These individuals are usually offered simple but well-paid and quick jobs during the recruitment process. As a rule, potential saboteurs are selected based on their ability to move freely around Europe, irrespective of any specific skills or training they may have.

Unlike conventional Russian intelligence agents, recruited saboteurs frequently complete only a limited number of tasks before being detained. Furthermore, they do not receive the promised financial payments or any support from Russia once they are arrested. In 2024, over 50 saboteurs and coordinators were apprehended in Europe, several of them were arrested following investigations by Lithuanian intelligence and law enforcement agencies.

By conducting sabotage operations, Russia almost certainly is trying to influence Western societies, increase distrust in state institutions, and force political leaders to weaken support for Ukraine. We assess the Kremlin is failing to achieve these objectives, particularly in Lithuania. According to public opinion polls, most residents of Lithuania support the state's commitment to continue supporting Ukraine, and Lithuania remains one of the most active supporters. Annual military assistance to Ukraine remains stable at no less than 0.25 percent of Lithuania's GDP.
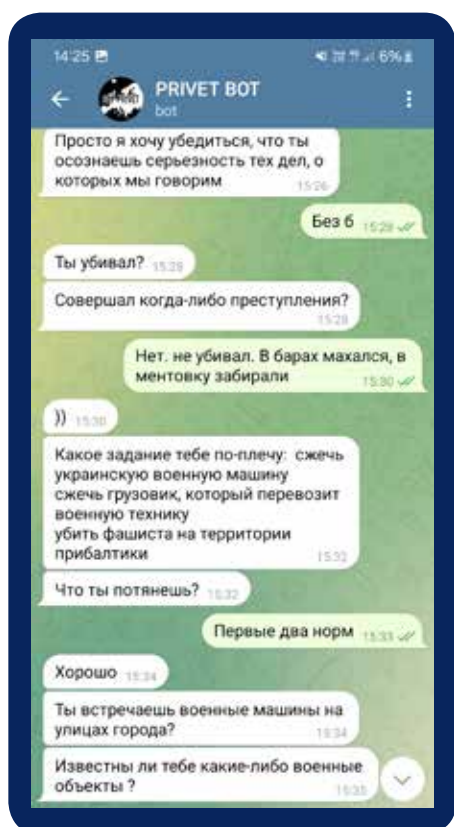
An example of recruitment in a *Telegram* group: the recruit is offered to set fire to a Ukrainian military vehicle, a truck carrying military equipment or to kill a 'fascist' in the Baltic States.

Source: *Organized Crime and Corruption Reporting Project*

Russian intelligence uses 'illegals' to collect sensitive information

In 2024, following an investigation by the VSD and Lithuanian law enforcement, a GRU 'illegal' was arrested in Lithuania. He was using his real identity but concealing certain aspects of his biography. The individual joined the Lithuanian Union of Political Prisoners and Deportees and the Homeland Union – Lithuanian Christian Democrats political party, emphasising the Soviet repressions his family had suffered. This gave him opportunities to collect intelligence.

The GRU used the 'illegal' to gather strategic intelligence on political processes in Lithuania and Europe. The GRU tasked him with gathering intelligence on Lithuanian defence, domestic and foreign policy, NATO consultations in Lithuania, preparations for military exercises, arms procurement, support for Ukraine, and high-ranking Lithuanian politicians' stance on international and domestic security policy.

The individual collected non-public, sensitive intelligence information by attending NGO and political events, making contacts with members of the above-mentioned organisations, and gathering information from open sources. He analysed the collected material and transmitted the data remotely via encrypted messages. The individual strictly followed conspiratorial security measures and used radio, computer, and software equipment provided by the GRU.

The 'illegals' program is a sophisticated, costly, and exclusive method used by Russian intelligence services to collect sensitive information. Individuals selected for the programme undergo a lengthy, specific training. They must be highly skilled in foreign languages, have a nondescript appearance, and be psychologically prepared to spend most of their lives abroad pretending to be someone else. 'Illegals' operate under false foreign nationalities or use their own, and over a long period of time they build up a coherent and convincing cover story which allows them to operate covertly in the West. Once placed in a foreign country, they graduate from universities, start families, and become involved in local communities. 'Illegals' lead seemingly ordinary lives and do a wide range of jobs, most often in business, academia, or the arts. After building a life free from suspicion, they conduct long-term, covert intelligence activities. Consistently crafted cover stories and their meticulous tradecraft make identifying Russian intelligence 'illegals' extremely difficult.

The Putin regime is confident of victory over Ukraine and the West

Russia's main objective in its war against Ukraine has not changed since 2014. It seeks to turn Ukraine into a dependent state and to compel Western democracies to acknowledge Russia's right to interfere in the internal affairs of its sovereign neighbours. Having failed to achieve its objectives through manipulation and influence operations against Ukraine, Russia chose to utilise military force in 2022.

Russia openly declares that peace with Ukraine is only achievable on its own terms, which state that both Ukraine and the West must accept defeat and acknowledge that Russia's aggression was lawful. A diplomatic solution to the conflict is unlikely, as this would simply see Russia return to the same stalemate that Vladimir Putin decided to reverse in February 2022 by attacking Ukraine. Russia's military measures are proving effective. This is demonstrated by Russia's regained confidence in its armed forces, the expansion of Ukrainian territories under occupation, and the destruction of Ukrainian infrastructure.

Russia has the resources to continue the war for years. In any democracy, such situation as the one in Russia would be regarded a disaster: massive human losses, problems in the financial system, economic stagnation in sectors unrelated to the military industry, and foreign trade sustainable only because of smuggling and shadow schemes. Nevertheless, the war is popular in Russia. In an authoritarian society, the results of public opinion polls may not be entirely reliable due to the fear of reprisals, but even the responses to a completely non-political question, "How are you feeling today?", are the most positive since 1994 (historical data show that the economic crises in 1998 and 2008 and the mobilisation in 2022 had a short-term negative impact on public opinion). Both the regime and most of the Russian population believe that the war in Ukraine is not against Ukrainians, but rather against the West. Although almost 60 percent of Russians believe that the war in Ukraine could escalate into a war with NATO, this likely only strengthens support for the war and the regime.

The Putin regime considers itself to be in full control of the political and social situation, and threats to its stability

are unlikely in the short term. Putin's perceived superiority over Ukraine-supporting Western democracies will drive his resolution to wage war and exert pressure on the West until he secures substantial concessions.

A `peace for land` solution to the conflict is also unlikely, as the annexation of Ukrainian territory is not an end goal for Russia, rather an instrument to legitimise and consolidate its aggressive policy. The Kremlin is forcibly Russifying the occupied Ukrainian territories because it has no intention of negotiating their return and highly likely is seeking to turn their inhabitants against a non-occupied Ukraine in the long term. Russification is not a bargaining chip for Moscow; it is an integral part of the destruction of Ukraine.

International pressure has no effect on Russia's position. Chinese support and sanctions evasion schemes mitigate the impact of international sanctions, while most of the Global South does not support Russia's policies but has no interest in breaking relations with it. Russia's attempts to build an anti-Western coalition have so far failed to produce substantial results. However, Russia's efforts to create alternative frameworks for economic and financial cooperation and to weaken confidence in existing international institutions and legal norms could have significant long-term implications for the evolution of the global order.

Russia's strengthening alliances with Iran and North Korea indicate a significant shift in Russian foreign policy. In its confrontation with the West, Russia is willing to collaborate with any ally or use any means available at its disposal. Russia views conflicts, such as those in the Middle East as well as supporting and arming authoritarian regimes, as an opportunity to expand its influence and divert the attention of its opponents. Russia has no intention of re-establishing its former relations with democratic countries. Even if the war in Ukraine ended or was frozen, threats emanating from Russia – military aggression, sabotage and influence activities – would persist. Moscow would only reconsider its priority targets. Prior to the invasion of Ukraine, Russia's demand that the West return to the 1997 NATO borders is indicative of this. The reason behind this ultimatum is to undermine the capacity of Central and Eastern European states to resist Russian influence and military aggression.

Despite growing risks to its economy, Russia can still finance the war

Russia's war of attrition against Ukraine requires enormous financial resources, and so far, the Kremlin has succeeded in finding them. Military spending has been growing every year at a staggering rate and will rise to 13.5 trillion roubles (around €120 billion) in 2025, amounting to 6.3 percent of GDP. It will be Russia's largest military budget since the collapse of the Soviet Union and nearly four times bigger than in 2021 – the last year before the invasion of Ukraine. It is almost certain that the actual spending on the war will be even higher, as Russia usually allocates additional funds from the classified part of the budget as well as other sectors (e.g. healthcare and education).

RUSSIA'S OFFICIAL MILITARY BUDGET 2021–2025
(trillion roubles unadjusted for inflation)

Year	Value
2021	3.6
2022	4.7
2023	6.4
2024	10.8
2025	13.5
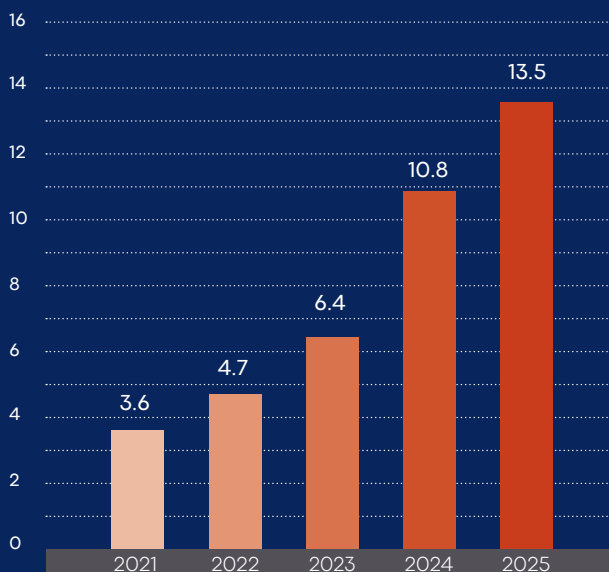
Russia has not yet reached the limit of its financial capacity. Untapped economic reserves give the government room for manoeuvre. As a result, it will not only be able to maintain a similar level of war funding in the near term but is likely to be able to increase it further. If necessary, the government could borrow domestically, raise taxes or introduce new ones (e.g. a windfall tax on the most profitable companies), and use the liquid assets of the National Welfare Fund. In addition, cutting expenses of the other segments of the federal budget could be another (albeit a politically sensitive) solution. A precedent has already been set – allocations for social services, which are among the regime's priorities, were cut by €11 billion (around 16 percent) in the budget of 2025.

'THE NEW ECONOMY'

The Kremlin declares that the military sector will be the engine of the 'new, independent and invulnerable' Russia's economy. For the Russian people, Putin promises development, which the country is supposed to achieve by fusing military and civilian industries and deepening partnerships with the Global South. For this reason, in 2024, the Kremlin moved to curb systemic corruption and created a new team of trustees to oversee military spending. In May 2024, Sergei Shoigu, a long-time defence minister and friend of Putin's, was replaced by the economist Andrei Belousov. Other top officials within the Ministry of Defence were accused of fraud or bribery. However, structural preconditions for a thriving economy in the authoritarian Russia do not exist as the war continues. Strict administrative measures are helping the Kremlin to increase the efficiency of individual projects or programmes, but there will almost certainly remain the priority for strengthening Russia's military power and regime's security. For Russia's neighbours, this will remain a source of threats.

However, high military spending also has a negative impact. The resulting growth of Russia's GDP is not sustainable. As the share of military spending within the national economy grows, Russia will find it increasingly challenging to reorient itself and return to a peacetime economic model. The military-industrial complex and the Russian Armed Forces (financially supported by the government) attract labour from other sectors.

Therefore, the overall productivity and competitiveness of the Russian economy is declining. So far, all these trends have not forced the Kremlin to change its foreign and security policy. Moscow is willing to absorb the rising costs to continue the war of attrition. It is highly likely that such course will make the country's economy weak, uncompetitive, and extremely vulnerable in the future.

Russia continues to strengthen its military power

Russia's ability to use military force against NATO countries is currently very limited, as most of its conventional capabilities are dedicated to the war against Ukraine. In the near term, Russia is likely to have sufficient human, financial, and military resources not only to continue fighting in Ukraine at a similar intensity but also to increase its military capabilities.

The development of military capabilities is a top priority for the Russian leadership, and they are allocating significant resources to it. Russia continues to pursue its ambitious military reform plans announced in 2022 which would see a 30–50 percent increase in the number of personnel, weapons, and combat equipment in the Russian Armed Forces in Western direction.

Although Russian officials claim that around 400,000 troops joined the Russian Armed Forces in 2024, the total number of military personnel did not grow so rapidly due to the heavy combat losses. As part of the military reform, Russia plans to increase the number of troops to 1.5 million. Given the current

trends in the growth of military personnel, this ambition is feasible and would allow Russia to fill the newly formed units with personnel.

Russia is also focusing on the development of its military industry. While Western sanctions have negatively affected Russia's military industry (lengthening supply chains for necessary components, increasing the cost, and reducing the quality of military production), the production volume of artillery shells, missiles, and other major categories of ammunition increases every year. The production of ammunition and new military equipment is important not only for the ongoing war but also for restoring the reserves of arms and ammunition that would be needed for a military conflict with NATO.

The further growth of Russia's military power will depend directly on the course of the war in Ukraine. A reduction in front-line needs could allow Russia to accelerate the build-up of new troops and increase reserves of arms and ammunition.

In the medium term, Russia is unlikely to be able to build up the capabilities needed for a large-scale conventional war against NATO. However, Russia may develop military capabilities sufficient to launch a limited military action against one or several NATO countries. This may encourage the Russian leadership to use military force in the mistaken belief that NATO should not be able to react in time and that Russia should be able to localise the conflict and bring it to a swift and favourable end.

Strengthening the Baltic defence and deploying allied forces on NATO's Eastern Flank are key factors in deterring Russia from military conflict in our region. This increases the costs of a potential military conflict to Russia and makes it less likely that such a conflict would be localised and would not involve the other members of the Alliance.

Temporarily reduced Russian military capabilities in Kaliningrad remain strong

To meet the needs of the military operation in Ukraine and to compensate for losses, Russia is transferring ground troops and combat equipment to Ukraine in large numbers – even from regions closest to NATO, such as the Kaliningrad Region. Naval and air components are less involved in the military action and are used to demonstrate force in the Baltic Sea region.

One of the main episodes of the military power demonstration in 2024 was the large-scale strategic command and staff exercise 'Okean 2024' conducted in September, during which the naval and air components played a key role. 'Okean 2024' also demonstrated that the A2/AD (anti-access and area denial) developed by Russia in the Baltic Sea region, and especially its air defence capability, although partially degraded, is operational and capable.

The military grouping in the Kaliningrad Region remains capable of performing essential tasks. However, its capacity to carry out landing tasks will remain limited in the medium to long term due to the deployment of landing craft to the Black Sea. The capabilities currently demonstrated by Russia in the event of a military conflict against NATO would not be sufficient to establish dominance but could disrupt NATO's actions in the Baltic Sea region.

Russia updated its nuclear doctrine

The nuclear power status is of paramount importance for Russia. It helps to ensure strategic deterrence, has great symbolic value, and provides additional options in foreign policy. By employing nuclear messaging, Moscow seeks to influence the decision-making of other states, thus protecting its interests from harmful consequences. For example, in May 2024, the Russian

Ministry of Foreign Affairs announced that it would use non-strategic nuclear weapons exercises to "cool down the hotheads in Western capitals". This was a reaction to the transfer of F-16 fighter jets to Ukraine and the statements by Western officials regarding the support for Kyiv.

Strategic deterrence is one of the key goals of Russia's security policy, and it involves the threat of both strategic non-nuclear weapons and the existing nuclear arsenal (strategic and non-strategic nuclear weapons). The effect is usually created by the rhetoric of officials and institutions, and by various actions related to nuclear or other strategic capabilities, which send Moscow's desired signals and messages: military exercises, introduction of a higher level of combat readiness in relevant units, deployment of warheads, strikes with strategic non-nuclear weapons, development of nuclear infrastructure, etc. The aim is to strengthen the deterrence and influence the decision-making processes of opponents in favour of Russia. For example, in the context of the war against Ukraine, Russia constantly manipulates its nuclear capabilities. In this way, it seeks to dissuade the West from becoming directly involved in the conflict and from providing military support for Kyiv.

During its war against Ukraine, Russia routinely makes similar statements and uses other means of nuclear messaging. The most important of these in 2024 was the revision of the nuclear doctrine. This document (made public in 2020) sets out the conditions under which Moscow can use nuclear

weapons. The Kremlin updated it and made it more relevant to Russia's current national security situation. Indirect but obvious references to NATO and Ukraine were included, but the most important change was the expansion of the list of conditions allowing the use of nuclear weapons.

A still from the video footage released on 29 October 2024 by the press service of the Russian Ministry of Defence. It shows a 'Yars' intercontinental ballistic missile being launched during a strategic deterrence exercise.
AFP / Scanpix

Russia's nuclear doctrine defines the conditions under which it can use nuclear weapons:

- If it obtained reliable information about the launch of ballistic missiles attacking Russia and/or its allies;

- If an adversary used nuclear or other weapons of mass destruction on the territories of Russia and/or its allies, as well as against Russian military formations and/or facilities located outside of Russia;

- If the actions by an adversary against the Russian state or military installations of critical importance disrupted the response of nuclear forces;

- In case of aggression against Russia or Belarus with the use of conventional weapons, imposing a critical threat to their sovereignty and (or) territorial integrity;

- If it obtained reliable information on the massive launch of air-space attack means (strategic and tactical aircraft, cruise missiles, unmanned, hypersonic and other aerial vehicles) and their crossing of the state border of Russia.

With these alterations, Russia theoretically expands its abilities to use nuclear weapons, but in practice, it retains the freedom to decide on a response. This is ensured by using vague wording (it is not clear what will be considered a massive air-space attack or a critical threat to the sovereignty or territorial integrity of the state). It is highly likely that the Kremlin is doing this deliberately while seeking to increase strategic uncertainty about its alleged red lines.

The Russian regime is increasing public and online surveillance

Russia is in the process of establishing a centralised video surveillance system with facial recognition and deploying artificial intelligence (AI) tools to monitor digital content. The official reason for developing these surveillance systems is to improve public security. However, such systems also help the regime to monitor and track down any form of dissent, censor online content, and hinder the formation of any opposition movement.

Russia's gradually emerging model of mass public surveillance has been frequently compared to China's social credit system, the world's most extensive digital control system. As part of this system, China uses a range of digital technologies to control people and analyse their personal data.

Russian citizens are finding it difficult to evade the regime control.
AP / Scanpix

Public surveillance

By 2030, Russia intends to integrate all public surveillance with facial recognition capabilities into a centralised data storage and processing system. Data captured by these cameras will then be analysed using facial and image recognition AI systems. In addition to monitoring public spaces, Russia collects biometric data for security and law enforcement agencies to later use them in their investigations.

Facial recognition technology has been integrated into the `Face Pay` biometric payment system, which is used for payments on the Russian metro network. Customers are required to link their photo with bank and metro cards to pay for the services. `Face Pay` was first launched in the Moscow Metro. In 2024, it was subsequently installed in six other Russian cities. It is planned that the technology will be used in all Russian metro stations by the end of 2025.

Internet surveillance

The Russian regime is set to deploy the Internet monitoring system, an integral part of the `RuNet` (the Russian segment of the Internet), with the aim of restricting the country's access to the global Internet and strengthening the oversight of the local Internet.

Internet monitoring systems, such as the AI-based `Oculus`, are used to monitor online content. These systems can recognise images, characters, faces, analyse online conversations, and identify the text present in photos and videos. `Oculus` is employed in Russia for the detection of online content that is prohibited by law, including extremist and pro-Ukrainian narratives, information about illegal events and gatherings, as well as information related to drugs, weapons proliferation, or LGBT+ issues.

BELARUS

■ Belarusian intelligence services exploit the Belarusian diaspora in Lithuania to establish long-term intelligence positions; they increasingly use remote communication tools to establish and maintain contacts with their agents.

■ Belarusian authorities are threatening the safety of Lithuanian citizens visiting the country. In addition to conducting interrogations and detentions, they also initiate legal proceedings against Lithuanian citizens for criticism of the Belarusian regime.

■ Following the 2025 Belarusian presidential election, which was neither free nor fair, Lukashenka has consolidated his power. In the near term, he will seek to be recognised as the legitimate leader of Belarus.

■ Unrestrained use of Belarusian airspace by the Russian Armed Forces poses a risk of incidents in neighbouring NATO countries. In September 2024, a Russian Geran-2 (Shahed-136) crashed in Latvia after crossing Belarus.

Belarusian intelligence services intensify activities against the Belarusian diaspora in Lithuania and increasingly detain Lithuanian citizens in Belarus

The sizeable Belarusian diaspora in Lithuania continues to present opportunities for Belarusian intelligence services to establish long-term intelligence positions in Lithuania. Belarusian intelligence services coerce members of the Belarusian diaspora into cooperation by threatening the security of their relatives remaining in Belarus and the right to use their own real estate or businesses in Belarus. Belarusian intelligence services are increasingly using remote communication tools to establish and maintain contacts with agents operating abroad; they are instructed to gather intelligence on Lithuanian institutions, the Belarusian diaspora, and the democratic opposition.

Belarusian intelligence targets Belarusian companies that have subsidiaries in Lithuania but continue to operate in Belarus. These companies are monitored by Belarusian intelligence officers who possess information not only on employees working in Belarus but also in Lithuania. Belarusian intelligence services pay close attention to individuals with even the slightest involvement in

opposition activities, with whom they remotely establish contact, apply pressure, and try to lure them back to Belarus. If these individuals return to Belarus, they are interrogated, often detained, and recruited by intelligence services.

Despite the risk of detention, Belarusians residing in Lithuania keep visiting Belarus. Belarusian intelligence services are screening Belarusian nationals at the border to identify individuals with anti-regime attitudes, those who participated in the 2020 protests or otherwise support the opposition. Furthermore, other Belarusian agencies and institutions collaborate with intelligence services by providing information on individuals of interest and their arrival in Belarus. Individuals of interest are then subjected to various forms of pressure, including threats and psychological coercion, in an attempt to force them to appear for questioning. During the sessions, officers not only seek to gather intelligence but also attempt to recruit. Belarusian intelligence services threaten the physical safety and security of Lithuanian citizens visiting

Belarus by acting in a manner that is incompatible with international law. They carry out intelligence interrogations and illegal detentions of incoming Lithuanian citizens for supporting the Belarusian opposition, followed by prosecution for their political views and criticism of the Belarusian regime. Belarusian intelligence and law enforcement authorities use extremely harsh methods and excessive force during detention.

Since 2023, Belarusian intelligence services have been building false cases against Lithuanian citizens with unfounded and politically motivated accusations. We assess that the Belarusian regime's actions are intended to exert pressure on Lithuania for it to reconsider its policy towards Belarus and to reinforce the narrative of a Belarus surrounded by hostile countries.

A Lithuanian citizen unjustly detained and put on trial in Belarus.
ONT film

A successful operation led to the arrest of two suspects spying for Belarus

In November 2023, a counterintelligence investigation that had lasted more than a year reached its climax. The pre-trial investigation based on information gathered by the AOTD led to the arrest of two Lithuanian citizens, a man and a woman (a couple), suspected of cooperating with the Belarusian military intelligence (GRU). They were accused of espionage under Articles 25(4) and 119(2) of the Lithuanian Criminal Code.

The suspects carried out Belarusian GRU tasks, gathering and transmitting information in various ways to a GRU officer for payment. To collect information, one of the suspects joined the Lithuanian Riflemen's Union. Belarusian intelligence was interested in information on Lithuanian and NATO military hardware and weapons deployed to Lithuania, the infrastructure of military units, Lithuanian strategic objects and means of their protection, activities and training content of the Lithuanian Riflemen's Union, and the preparedness for defence during an armed conflict. The preparations and security measures during the NATO Summit in Vilnius, activities of the Belarusian opposition in Lithuania, and potential targets for recruiting were also of interest to Belarusian intelligence. Although the information collected by the above-mentioned persons was unclassified, the Belarusian and Russian Armed Forces need it to prepare plans for military aggression and other hostile activities against neighbouring countries.

The investigation by Lithuanian officials provided valuable information on the methods, techniques, and means of operation of the Belarusian GRU, including recruiting, communication, and transmission of information. The investigation revealed the use of conspiratorial premises, schemes of payment, and contribution of Belarusian citizens and former state officials in supporting operations carried out by Belarusian intelligence services.

This case once again confirms that any Lithuanian citizen may become a target of hostile intelligence services, even without having access to classified information. Recruitment is executed in various ways, including blackmailing and taking advantage of a person's vulnerabilities, such as poor financial situation, addictions, or ideology. Belarusian intelligence services also use former Belarusian civil servants, law enforcement and security officials for recruiting or other assistance.
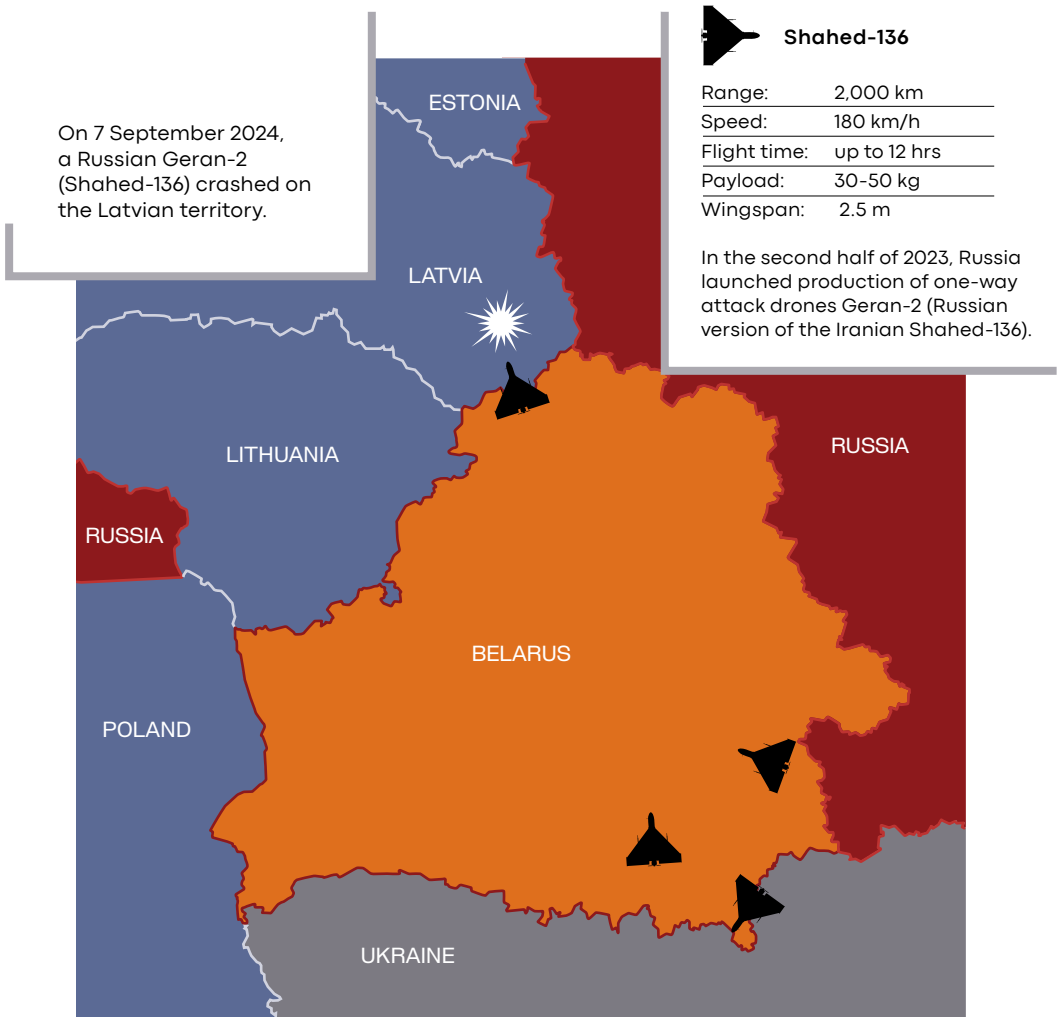

Personal belongings and a firearm found during the arrest of a suspect.
AOTD photo

Unrestrained use of Belarusian airspace by the Russian Armed Forces poses a threat to neighbouring NATO countries

Currently, there are no Russian ground manoeuvre units in Belarus, but Russia continues to use Belarusian airspace freely. Since July 2024, the Russian suicide drones Geran-2 (Shahed-136) have been flying through Belarusian

On 7 September 2024, a Russian Geran-2 (Shahed-136) crashed on the Latvian territory.

Shahed-136

Range:	2,000 km
Speed:	180 km/h
Flight time:	up to 12 hrs
Payload:	30-50 kg
Wingspan:	2.5 m

In the second half of 2023, Russia launched production of one-way attack drones Geran-2 (Russian version of the Iranian Shahed-136).

Since July 2024, Russian suicide drones Geran-2 (Shahed-136) have been flying repeatedly through Belarusian airspace to Ukraine.

airspace to Ukraine. Some of the drones cross Belarusian airspace and fly to Ukraine, while others enter Ukrainian airspace from Russia, fly to Belarus and return to Ukraine. However, some drones deviate from their route and pose a threat to NATO countries bordering Belarus. In September 2024, a Russian Geran-2 (Shahed-136) crashed on the Latvian territory after crossing Belarus.

The Belarusian Air and Air Defence Forces rarely respond to the flights of

the suicide UAVs that enter Belarusian airspace. There are established cases of Russian Geran-2 (Shahed-136) shoot-downs by the Belarusian Armed Forces, but Belarus either does not reveal the identity of the downed drones or does not publish the incident reports. The Lukashenka regime avoids commenting further on Russian drone flights over the Belarusian territory, as the threat posed by drones to Belarus contradicts its public communication on the security of the country.

Re-elected Lukashenka consolidates the authoritarian regime

The 2025 presidential elections in Belarus were neither transparent nor democratic, but they were nevertheless essential for Alexander Lukashenka to legitimise his rule in the eyes of the Belarusian public and the international community. The Belarusian regime sought to create an illusion of democratic elections, but with the pre-selected pro-regime candidates and the announcement of the election date only three months prior, the elections resembled a farce. The elections were

organised in such a way that the public had as little time as possible to engage in any anti-regime civic initiatives.

In the run-up to the presidential elections, the regime proactively sought to prevent a repetition of the 2020 mass protests and to rally support by using 'carrot and stick' tactics. It continued to carry out severe public repression, targeting not only potential opposition figures but also Belarusian citizens who participated in the 2020 protests.

Concurrently, the regime initiated a series of events designed to garner public support, including the 'Unity Marathon' campaign, which was run by Lukashenka's daughter-in-law (the wife of his son, Dmitry Lukashenka) and spanned for several months encompassing concerts, exhibitions, and other events in all major cities of Belarus.

Lukashenka regards Russia as a key supporter of his regime and a key guarantor of his power. As soon as the date for the Belarusian presidential elections was announced, Russia confirmed its support for its closest ally in the event of mass protests.

Lukashenka was elected for his seventh term as president of Belarus, further consolidating his power. The pro-regime party 'Belaya Rus' holds almost half of the seats in the House of Representatives (the lower house of the parliament), while the Council of the Republic (the upper house of parliament) is occupied by Lukashenka's closest confidants, such as the Speaker of the Council of the Republic, Natalia Kochanova. According to legislation, the president can be impeached by the All-Belarus People's Assembly for violations of the Constitution, treason, or other serious crimes. However, in April 2024, Lukashenka was elected as the chair of this body. By eliminating any potential political opposition within Belarus and ensuring that state institutions were free from any anti-regime dissent, Lukashenka reorganised the political structure of Belarus to ensure the stability of his regime.

Belarus' foreign policy becomes subservient to Russia's foreign and security policy

Belarus is providing increasing support for Russia's international policy initiatives, particularly in the context of establishing an alternative international order and a multipolar world. Public statements made by Belarusian officials to the international audiences emphasise the necessity for a new Eurasian security architecture. Belarus advocates that the consolidation

of Russian-led regional organisations, the establishment of the new ones will facilitate the realisation of this objective.

Belarus is a key ally in Russia's foreign policy, aligning its strategic documents with Russia's international security interests. For example, in spring 2024, Belarus updated its military doctrine, adopting a more assertive stance. The new doctrine, unlike the 2016 version, is openly hostile towards the West, stating that the US, NATO and the 'collective West' are fuelling international confrontation to maintain world dominance. This aligns with Russia's perspective that the war in Ukraine was provoked by the 'collective West' and that international organisations are instruments of the West. It highlights that by hindering a peaceful resolution to the conflict in Ukraine, the West is creating conditions that could lead to an escalation of the conflict and the involvement of NATO. The document does not refer to Ukraine as an independent entity in international relations. We assess that the new doctrine reiterates Belarus' full support for Russia in its war against Ukraine and, if necessary, for actions against NATO.

In the near term, Lukashenka will seek to be recognised as the legitimate leader of Belarus and pursue pragmatic interests in developing relations with Western countries, including Lithuania. However, Belarus will remain Russia's closest ally and will not change its strategic direction.

CHINA

■ China provides Russia with essential dual-use equipment and technologies, which enable Russia to maintain initiative on the battlefield and continue the war of attrition. China's stance on supporting Russia is based on the notion that the Russian regime should not lose the war.

■ The war in Ukraine serves China's interests by draining the West's resources, fuelling internal divisions and forcing Russia to accept terms of cooperation favourable to China.

■ China is trying to secure an access to Western technologies through a combination of espionage and cooperation with Western academia.

■ China highly likely remains interested in Lithuania's scientific achievements, especially in the fields of lasers, semiconductors, and biotechnology, i.e. research which is in line with China's strategic priorities.

China is helping Russia to continue its war against Ukraine

The ongoing war in Ukraine aligns with Beijing's interests as it presents a challenge to the West, diverts its attention, drains its resources and fuels internal divisions. China's support for Russia is driven by their shared opposition to the West and the fact that Russia's war-related setbacks force the Kremlin to accept terms of cooperation more favourable to China. We assess that China's current stance on supporting Russia is driven by the belief that the Putin regime should not lose the war.

At the start of Russia's invasion of Ukraine, China faced challenges in finding a balance between its partnership with Moscow and engagement with the West. However, China has demonstrated a capability to adapt its foreign policy in a manner that aligns with its strategic interests. While Beijing fully supports Moscow, it has taken measures to conceal the most sensitive details of this cooperation, thereby achieving a degree of success in evading secondary sanctions. At the same time, China has been projecting an image of a neutral country interested in a peaceful resolution of the conflict on the global stage.

China and Russia are strengthening their military cooperation. China's provision of essential dual-use equipment and technologies is enabling Russia to reconstitute and develop its military capabilities, thereby maintaining the initiative on the battlefield and the war of attrition. This arrangement almost certainly is mutually beneficial, as it allows Russia to manufacture necessary armaments domestically, while China is avoiding criticism and sanctions that it could face if it openly supplied weaponry to Russia. This cooperation also allows China to acquire Russian technologies. Over the decades China has increased its efforts to modernise the defence industry and has become increasingly capable of independently producing advanced fighter jets, warships, and other key military equipment. However, China's defence industry still relies on Russian-made engines for its aircraft. Beijing is also interested in other areas related to advanced military technologies.

China still values its political and economic relations with the West and in order to maintain these ties, Beijing is concealing its cooperation with Russia's

military industry. China portrays that it is restricting the collaboration of some Chinese private companies with Russia's defence industry, but it is highly likely that those restrictions are only imposed on the cases that become public and harm China's international reputation.

Trade between China and Russia is on the rise, helping Moscow to mitigate the impact of sanctions and sustain its economy. Since Russia's full-scale invasion of Ukraine, trade volumes between China and Russia have grown, with the annual growth rate amounting to approximately 30 percent. Russia is importing goods from China that have become unavailable due to sanctions, including cars, industrial and agricultural equipment, and electronics. Russia's major exports to China primarily consist of raw materials and agricultural products.

Energy cooperation between the two countries is also intensifying, which is helping Russia to compensate for lost sanction related revenues from energy trade. Since the beginning of the war, Russia has become China's primary oil supplier, delivering crude oil to China at discounted prices. In addition, China has been increasing its imports of Russian natural gas via pipelines by

approximately 20 percent annually and expanding liquefied natural gas transportation through the Arctic, where it has invested in Russian projects. This cooperation model is beneficial to China as it allows the country to acquire cheaper energy resources, expand its interests in the Arctic, and force Russia to assume greater commitment to projects developed jointly.

Chinese financial institutions help to support the stability of Russia's financial system. By integrating Russian banks into its CIPS (Cross-Border Interbank Payment System), China has provided a crucial lifeline to Russia, following its disconnection from the SWIFT system. Since the start of the war, there has been a significant surge in the use of the yuan for bilateral transactions. Russia conducts about a quarter of its settlements with third countries through Chinese banks using the yuan.

Political ties between China and Russia are becoming increasingly institutionalised, enabling both countries to expand and strengthen their cooperation. Since the war in Ukraine began, Chinese President Xi Jinping and Putin have had two state-level meetings, along with numerous other meetings on the sidelines of international

forums. During these meeting both leaders always referred to the necessity of strengthening bilateral relations in security, defence, transport, finance, trade, energy, technology, education, and other areas. Meetings between lower-level Chinese and Russian officials responsible for policy implementation are also becoming more frequent and regular. China and Russia undoubtedly coordinate and support each other's interests in the UN, BRICS, the Shanghai Cooperation Organisation, and other international organisations. International events organised by China serve as an international platform for Russia.

China highly likely will alter its opinion on the war in Ukraine in the near term, which is the basis for its decision to support Russia. As a result, the nature, scope, and tactics of this support are likely to remain unchanged, thereby significantly strengthening Russia's ability to continue the war and increasing its dependency on China.

China engages in technological espionage to accelerate economic growth and modernise its military

In order to increase its economic competitiveness and accelerate military modernisation, China is seeking to secure access to Western technologies and the expertise required to develop them. Strategic documents and plans openly outline China's technological needs and specific areas for development. For instance, the 'Made in China 2025' plan sets ambitious goals to achieve breakthrough in high value-added industries, including the new information technology, aerospace and aviation sectors, railway, renewable energy, biotechnology, electronics, industrial machinery and robotics, maritime, medicine, and industrial agriculture.

China collects information on technologies developed by the West through a combination of espionage and lawful means. Beijing funds joint research with foreign scientists, establishes collaborative research laboratories with foreign universities, and runs talent recruitment programmes to attract experts to China. It also forms joint ventures with international companies.

THE 'SEVEN SONS OF NATIONAL DEFENCE',

leading Chinese universities closely associated with the country's defence industry

- Harbin Institute of Technology
- Harbin Engineering University
- Beijing Institute of Technology
- Beihang University
- Northwestern Polytechnical University
- Nanjing University of Science and Technology
- Nanjing University of Aeronautics and Astronautics

The objective of China's civil-military fusion strategy is the integration of civilian technologies into the Chinese Armed Forces. A number of Chinese universities play a role in this strategy by conducting research on weapon development and the application of technologies in the military. The Chinese regime exploits these institutions and their international academic collaboration for technological espionage and covert technology transfer. Some of these universities are also trying to establish relations with Lithuanian research institutions.

Despite poor bilateral relations, China highly likely remains interested in Lithuania's scientific achievements, with particular focus on lasers, semiconductors, and biotechnology. Chinese scientists are particularly keen on collaborating with their Lithuanian counterparts in the fields of natural and technological sciences, including physics, astronomy, chemistry, environmental science, and materials engineering. Research in these fields is in line with the priorities outlined in China's strategic documents.

It is highly likely that Chinese universities with ties to the defence industry will seek to strengthen scientific cooperation with Lithuania by signing collaboration memorandums, initiating joint research projects, establishing laboratories, and offering internships or exchange programmes for researchers. It is possible that Chinese intelligence services will target representatives of Lithuanian academic institutions participating in various internship programmes.

INFLUENCE ACTIVITIES AGAINST LITHUANIA

■ Russia is trying to discredit Lithuania by accusing it of historical revisionism, supporting Nazi ideology, and inciting Russophobia. By accusing Lithuania of discrimination against Russian speakers and marginalising Russia's supporters, Russia seeks to attract the attention of international human rights organisations or other countries.

■ Chinese and Russian intelligence services use their cyber capabilities to conduct ongoing espionage campaigns and to gain new access to the information systems of Lithuanian state institutions. To facilitate the process of gaining access to the systems, hackers use psychological manipulation to affect users of the systems.

■ Foreign intelligence services are also looking for new ways to increase the efficiency of their malicious operations: they are adopting methods used by hackers from the criminal world, applying artificial intelligence tools, and attacking more often the cloud infrastructure used by the organisations they target.

Russia seeks to discredit Lithuania, increasingly accusing it of rewriting history, promoting Nazism, and spreading Russophobia

Russia's propaganda targeting Lithuania is centred on accusations of historical revisionism, support for Nazi ideology, and fuelling Russophobia. We assess that the Kremlin is seeking to tarnish Lithuania's image in the international arena, to justify Russia's geopolitical interests in the region, and to discredit Lithuania's anti-Soviet resistance.

A large and coordinated network of Russian propaganda instruments, consisting of state-controlled media, social networks and pro-Russian websites, ensures dissemination of narratives that discredit Lithuania. We assess that Russia is most actively using the *Telegram* app to conduct its propaganda and disinformation campaigns. To support the dissemination of propaganda, Russia's information policymakers use bots (automated profiles) and troll networks as well as targeted advertising. Disinformation campaigns typically follow a tried-and-tested model: initial provocative information is posted on an obscure website or social media account, and then disseminated by prominent *Telegram* channels with high follower counts, thereby amplifying its reach. To reach a wider audience, the information can be translated into several languages. Such information operation was conducted in May 2024, when pro-Russian *Telegram* channels disseminated fake information claiming that two individuals known for their anti-NATO stance had been allegedly detained in Lithuania on 9 May 2024. This information was subsequently circulated on Russian news websites and pro-Russian Lithuanian websites.

A key element of Russia's information policy against Lithuania is portraying it as one of the most Russophobic countries in Europe. This narrative is mainly based on the assertion that Lithuania discriminates against Russian-speaking people and seeks to marginalise Russia's supporters, irrespective of their nationality. Russia draws parallels

between this alleged Russophobia and genocide, suggesting that Russians in Lithuania and the other Baltic States are currently experiencing what Jews did during the Second World War. We assess that Russia likely accuses Lithuania of discriminating against Russian speakers to attract the attention of international human rights organisations and the support of countries highly sensitive to ethnic, cultural, and linguistic issues.

Maria Zakharova, the Russian Foreign Ministry spokeswoman, is known for making accusations against the Baltic States of alleged prosecution of Russian speakers.
IMAGO / SNA / Scanpix

The manipulation of historical memory constitutes an important element of the Kremlin's confrontational policy. The Kremlin supports historical initiatives that discredit Lithuania and the other Baltic States, thereby legitimising history interpretations that serve Russia's interests. These initiatives aim to disseminate a narrative that accuses the Baltic States of systematically distorting the Second World War history, promoting Nazi ideology, and glorifying Nazi collaborators. The initiative 'With no Statute of Limitations' running for several years and aimed at the Russian public, supports this narrative. Under the auspices of this initiative, Kremlin-linked institutions implement various projects that supposedly expose the Baltic States as history revisionists.

In 2024, as Russia commemorated the 80th anniversary of the so-called liberation of Europe from Nazi Germany occupation, the Kremlin widely implemented various projects discrediting Lithuania and its anti-Soviet resistance. In 2025, when Russia commemorates the 80th anniversary of the end of the Second World War, the number of Russian history policy and propaganda initiatives against Lithuania and the Baltic States will increase.

Artificial intelligence tools are used to generate misleading content

Generative AI tools, including deepfakes (video, images, audio) and text generation, offer the potential to create digital content faster, more cost-effectively, and with less human intervention.

AI tools intended for content generation are not necessarily regarded as a threat. However, they can accelerate dissemination of disinformation and discredit on political systems, media, or electoral processes. Until 2024, the impact of AI-generated content was relatively limited, but with ongoing technological developments AI-generated disinformation highly likely will become more effective and harmful.
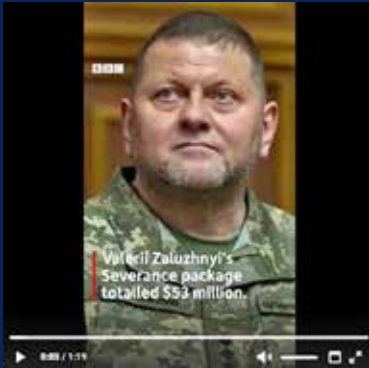
Video and image deepfake

Deepfakes generate reality-distorting images, photos, and videos. They can be used to create false impressions of political figures, for example, by making them appear to slander others or promote ideas that do not align with their actual agenda. These tools are easy to use, and the identities of their authors are easily concealed.

In March 2024, a video deepfake, mimicking a *BBC News* report and purportedly quoting *Bellingcat*, contained information that Valery Zaluzhny supposedly was paid a large sum of money to give up his political ambitions and leave Ukraine.

Audio deepfake

Voice deepfakes, which imitate the voice of family members or celebrities, are very convincing and almost undetectable. Any voice discrepancies in audios generated by AI tools can be explained by communication interference or poor sound quality. Voice cloning is most often used for generating unrealistic content in phone calls, radio recordings, and interviews.

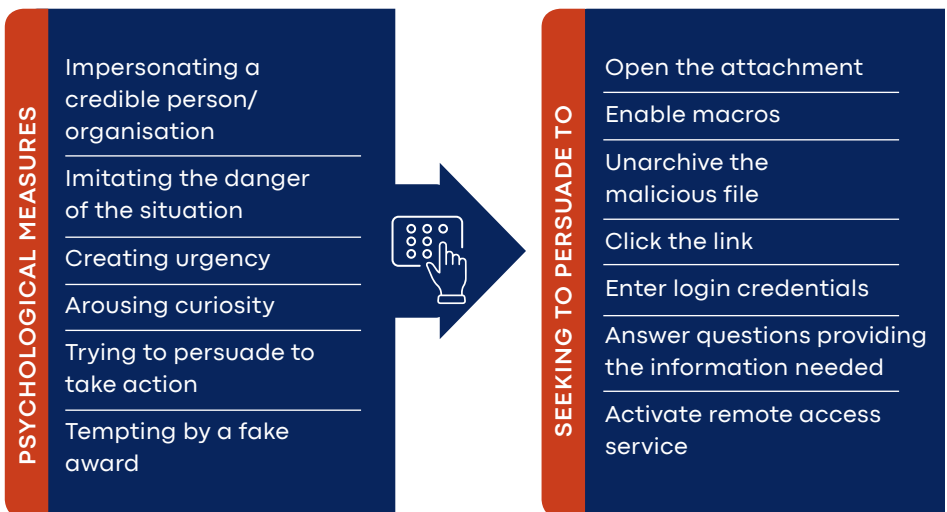## Chatbots and text generation

AI-generated chatbots, such as *ChatGPT*, can be used for creating texts in foreign languages and adapting them to different target audiences. They can be employed for writing fictitious social network posts, creating personal profiles or cover stories, and for engaging in virtual conversations with social media bots.

China-linked bot accounts on the social network *X* aimed at influencing the 2024 US presidential elections while Joe Biden was still running for president. These accounts spread disinformation on a range of issues, including migration policy, racial discrimination, and other topics.

The growing influence of AI on cybersecurity threats

The official and personal information systems of Lithuanian public sector employees continue to be targeted by cyber capabilities of Chinese and Russian intelligence services. Cyber espionage groups controlled by Chinese and Russian intelligence services are engaged in ongoing espionage activities and are attempting to gain new access to target information systems. It is highly likely that hostile states will remain motivated and will attempt to intercept information using effective and low-resource-requiring cyber tools in the near and medium term.

Although access to systems can only be gained through technical means, the human factor remains the biggest vulnerability, and hostile intelligence services actively exploit it. By manipulating people's emotions, they persuade users of information systems to perform actions that allow hackers to gain access to the information they seek or to the systems where data is stored. Hackers use various psychological tools to create an emotional impact that reduces people's attentiveness and critical thinking.

PSYCHOLOGICAL MEASURES

- Impersonating a credible person/organisation
- Imitating the danger of the situation
- Creating urgency
- Arousing curiosity
- Trying to persuade to take action
- Tempting by a fake award

SEEKING TO PERSUADE TO

- Open the attachment
- Enable macros
- Unarchive the malicious file
- Click the link
- Enter login credentials
- Answer questions providing the information needed
- Activate remote access service

Chinese and Russian intelligence services are looking for new methods to gain illegal access and carry out malicious activities themselves while also adopting successful tactics from criminal hackers, who are motivated by financial gain. Therefore, the range of their methods increases and makes it more difficult for investigators to distinguish between malicious state actors and criminal hackers. It is highly likely that all actors involved in illegal activities in cyberspace will use the proven models of malicious cyber activity as well as look for new approaches.

Hostile intelligence services use both psychological techniques and AI tools for cyber espionage operations.
PA Wire / PA

It is highly likely that the newly developed technologies will significantly change the cyber security landscape. For instance, there are more opportunities to use AI for cyber-attacks: from writing and customising a text to creating and modifying a malicious code. AI is also being trained to identify vulnerabilities in IT systems. Moreover, AI tools create additional security vulnerabilities. It is likely that the use of AI for malicious activities will grow in the near term, not only because of wider use of AI tools in society but also due to new ways to use this evolving technology in order to increase the effectiveness of cyber-attacks.

Technological development creates new challenges in taking responsibility for cybersecurity. Since organisations increasingly use cloud services, they tend to believe that it is the service providers' primary responsibility to ensure cybersecurity. Without organisations themselves taking steps to actively address cybersecurity practices of their employees and the implementation of safeguards such as dual authentication and access control, it is likely that the use of cloud services will remain vulnerable to malicious activity.

As the use of cloud services is growing, hostile intelligence agencies are looking for vulnerabilities in cloud infrastructure to exploit. For example, it was identified that APT29, a group linked to the Foreign Intelligence Service of the Russian Federation (SVR), targeted insufficiently secured cloud service accounts and managed to gain access to the infrastructure of cloud service providers, thus gaining long-term access to the target's data.

CRISIS REGIONS

■ The geopolitical divisions in the Middle East are altering the balance of power to Iran's disadvantage. The 'Axis of Resistance', which consists of groups loyal to Tehran, has faced significant setbacks. Tensions in the Middle East very likely will continue to be high due to the ongoing conflict between Israel and the 'Axis of Resistance', alongside the renewed fighting in Syria.

■ Instability in Africa is exacerbated by the expansion of radical groups in the Sahel and the ongoing war in Sudan. Russia is increasing its engagement in Africa with a low-cost, high-impact strategy. In this way, Russia seeks to strengthen its position in the geopolitical confrontation with the West.

Tensions in the Middle East are expected to remain high due to ongoing geopolitical tensions

Following the attack on Israel by the Palestinian terrorist group Hamas on 7 October 2023, tensions in the region escalated, leading to further geopolitical divisions. In response to continued attacks by Lebanon's Hezbollah, Israel launched a military operation against the group. It succeeded in destroying a large part of Hezbollah's arsenal and in eliminating most of its commanders, including its leader Hassan Nasrallah. In neighbouring Syria, the rebels

Israeli tanks return from Southern Lebanon on 4 December 2024 after a ceasefire between Israel and the Iranian-backed Hezbollah.
REUTERS / Scanpix

resumed their offensive at the end of 2024, overthrowing the authoritarian Assad regime (supported by Russia and Iran), which had ruled the country for more than half a century.

These events drastically shifted the balance of power in the Middle East. The position of Iran and the unofficial coalition it leads, the `Axis of Resistance`, has weakened. The ability of this coalition to undermine Israel and Western interests in the region is severely constrained.

A weakened pro-Iranian wing, the end of the civil war in Syria, and the Israeli ceasefire with Hamas and Hezbollah are the preconditions for a more stable situation in the Middle East. However, the `Axis of Resistance` is not defeated and almost certainly will look for opportunities to confront Israel and the West more actively in the future. The ceasefire in Gaza is fragile and does not address deeper causes of the long-standing conflict. In civil war-torn Syria, the political and security situation remains complex, with divergent interests and visions for the future of the country among various rebel groups. For these reasons, tensions in the Middle East in the near term will remain high.

Iran increasingly targets its adversaries in Europe

The Iranian regime is using members of European criminal gangs to target Iranian opposition figures and their supporters residing in Europe, as well as the objects linked to Israel or the Jewish community, in order to avoid attribution. The Iranian regime likely is seeking to intimidate opposition groups following the mass protests in Iran in 2022–2023, and to retaliate for the losses experienced by Iran and its allies in the Middle East.

Iran and its hired criminals have been responsible for a series of attacks across Europe, including in Greece, Spain, Germany, Sweden, the UK, and Denmark, which have involved violence, vandalism, explosives, and firearms. As Israel continues its military operations in the Middle East and directly confronts Iran, there has been an increase in attacks against Israeli embassies, some of which are linked to Iran. These attacks and Iran's efforts to intimidate adversaries are likely to pose a significant security challenge to Western countries in the near term.

ATTACKS LINKED TO THE IRANIAN REGIME IN 2023 AND 2024

On 9 November 2023, Alejo Vidal-Quadras, former MEP and supporter of the Iranian opposition, was shot in Madrid

On 31 January 2024, an unexploded grenade found outside the Israeli Embassy in Stockholm

On 17 May 2024, shots fired at the Israeli Embassy in Stockholm

On 1 October 2024, shots fired at the Israeli Embassy in Stockholm

2023

2024

On 4 December 2023, an attempted arson attack at the office of the National Council of Resistance of Iran in Berlin

On 29 March 2024, an *Iran International* journalist Pouria Zeraati was stabbed in London

On 6 June 2024, an assassination attempt on Siamak Tadayon Tahmasbi, an Iranian opposition figure, in Haarlem, the Netherlands

On 2 October 2024, two grenades exploded outside the Israeli Embassy in Copenhagen

On 28 March 2023, two people arrested in Athens for plotting an attack against a Jewish community centre

Growing instability and third-country influence in Africa

African countries face a growing risk of upheaval, instability, armed conflict, social unrest, and terrorist attacks. Instability is particularly acute in the Sahel region. Attacks by radical Islamist groups continue in Mali, Burkina Faso, and Niger; they are likely to spread to other West African countries. Citizens of Western countries in the Sahel are at risk of being kidnapped by groups linked to Al-Qaeda (AQ) and the Islamic State (ISIL).

Sudan is in the second year of a large-scale war that caused a major humanitarian crisis, with increased poverty, the risk of famine, and the number of refugees reaching 11.5 million in the second half of 2024. Despite its humanitarian consequences and the impact on the stability of the region, this conflict has received little attention from the international community. With two military factions competing for power, an end to the conflict is highly unlikely. The de facto break-up of the country cannot be ruled out, which would not only exacerbate the humanitarian crisis but also pose the risk of increasing migration to Europe.

African countries are becoming significant geopolitical actors because of their natural resources, growing market, and position in international organisations. As a result, global powers are expanding their ties with African countries. For instance, China focuses on stable economic cooperation, investment, trade, and long-term diplomacy. Russia is stepping up its engagement by offering security cooperation to African countries. It is pursuing a proven low-cost, high-impact strategy while exploiting instability, supporting coups and military regimes. The African Corps under the Russian Ministry of Defence is taking over private military companies operating in Africa. Moreover, Russia is actively spreading disinformation and propaganda against the 'colonial' West and portraying itself as fighting for the sovereignty of African states and a more fair multipolar world order. In this way, Russia seeks to strengthen its position in the geopolitical confrontation with the West, gain allies, and reduce its international isolation.

The bronze statue of Yevgeny Prigozhin (left),
leader of the Wagner mercenary group, and
Dmitry Utkin (right) in front of the `Russian
House` in Bangui (Central African Republic).
AFP / Scanpix

TERRORISM

■ The terrorist threat in Europe remains significant. International terrorist organisations are exploiting the conflict in the Middle East for propaganda purposes, spreading anti-Western propaganda, inciting anti-Semitism, and encouraging Muslims to engage in Jihad.

■ Islamist online propaganda has an impact on the terrorist threat in Lithuania. There is a constant risk that easily radicalised individuals in Lithuania may adopt extremist views and engage in extremist activities.

■ Lithuania is facing a risk related to the spread of right-wing extremist ideology among young people. In 2024, a group of right-wing extremists whose members were suspected of systematically committing violent hate crimes was disbanded.

Terrorist threat to Europe remains high

The terrorist threat to Europe remains significant due to the ongoing conflict in the Middle East, which terrorist organisations such as ISIL, AQ, and others are actively exploiting for their propaganda purposes. The Islamist propaganda disseminates anti-Western narratives, fosters anti-Semitism in

Officers escort a Syrian national suspected of carrying out a terrorist attack in Solingen, Germany, in August 2024.
REUTERS / Scanpix

Europe, incites violence against Jews, exacerbates societal polarisation, and encourages Muslims residing in the West to engage in Jihad.

In 2024, five attacks were carried out in Switzerland, Germany, and France; and dozens more were planned but prevented. Law enforcement agencies carried out arrests of individuals for disseminating extremist content or propaganda, terrorist financing, and other terrorism-related activities. It is highly likely that terrorist attacks planned or carried out in Europe in 2024 against the Jewish community or Israeli citizens were inspired by Islamist propaganda, as a "revenge against Jews, Christians, their allies in the US, Europe, and around the World for people of Gaza".

ISIL and AQ are experiencing difficulties in rebuilding their capabilities for coordinated attacks in Europe. Instead, these groups are focusing their efforts on online radicalisation and incitement, with the aim of motivating their Muslim supporters in the West to perpetrate attacks using easily obtainable resources, such as knives, machetes, firearms, vehicles, and arson. The Islamic State-Khorasan Province (ISKP) is currently regarded as one of ISIL's most capable branches. Operating in Afghanistan, Central Asia, and the North Caucasus, it has presence in both Asia and Europe, where it actively recruits. Individuals associated with ISKP have unsuccessfully attempted to carry out several terrorist attacks in Europe. Its ability to exploit and radicalise Central Asian diaspora in Europe makes ISKP a major threat to the EU.

Encrypted messaging apps, social media, and video platforms are the main tools used by terrorist organisations to disseminate extremist content and recruit followers, especially youth.

Propaganda of right-wing extremist ideologies draws young people into violent hate crime groups

As a majority of Western countries, Lithuania is facing a risk related to the spread of right-wing extremist ideology among young people who become involved in extremist activities for a variety of reasons, including a fascination with violence, a desire for social recognition, or a search for adventure.

The radicalisation of young people typically starts online, where they join public social media groups that disseminate radical video material, such as extremist 'memes' or video clips openly depicting violence. The next stage is often the progression to smaller and more organised, frequently closed social media groups. Prior to joining them, potential members may be requested to disclose their identity and fill in questionnaires regarding their ideological attitudes, knowledge, skills, and motivation.

Members of these closed groups share information on extremist activities, as well as instructions on how to manufacture improvised weapons, incendiary, and explosive devices. They also share personal data of ideological opponents. New members are often encouraged to extend their activities beyond the online environment to real-life scenarios. Initially, they are encouraged to commit minor offences, such as putting up posters or stickers in public spaces with the group's social media account links. Subsequently, they are persuaded to commit more complex crimes. This form of persuasion is particularly effective on minors, who often perceive losing social acceptance as a greater threat than the legal liability for their criminal actions.

In September 2024, a group of young right-wing extremists was dismantled in Lithuania. The group, which included minors, was suspected of systematically committing violent hate crimes targeting Asian and African nationals, ethnic minorities, and perceived ideological opponents.

Terrorist trends in other European countries indirectly impact on the situation regarding terrorism-related threats in Lithuania. Although Islamist groups or extremist individuals with the intention of carrying out terrorist attacks are not active in Lithuania, Islamist propaganda online poses a constant risk that easily radicalised individuals in Lithuania could adopt extremist views and engage in extremist activities.

In the near term, the threat of Islamist terrorism in Europe is highly likely to remain high due to the ongoing conflict in the Middle East, which is encouraging radicalisation among some Muslims. In the near term, lone extremists are likely to carry out attacks in European countries using their own resources and capabilities in public places against gatherings or officials as well as targets associated with Israel and the Jewish community. The likelihood of terrorist attacks organised by radical individuals in Lithuania will remain low in the near term.

2016

11th Army Corps is established in the Kaliningrad Region

At the NATO summit in Warsaw, the Alliance agrees to enhance NATO's military presence in Lithuania, Estonia, Latvia, and Poland

2015

Charlie Hebdo shooting

Illegal migration crisis in Europe reaches its peak

Islamic State attacks in Paris

Lithuanian intelligence foils FSB operation to infiltrate Lithuanian state institutions, including the Office of the President

2017

Russian bombers conduct first post-Cold War air strikes near Lithuania during Zapad 2017 military exercise

2018

The GRU attempts to poison Skripal and conducts an operation against the OPCW

Western allies expel more than 150 Russian intelligence officers operating under diplomatic cover

2019

Lithuanian intelligence issues its first public warning about hostile Chinese intelligence activities

For the first time, Lithuania does a spy swap with Russia

2020

COVID-19 pandemic starts

Amendments to Russian constitution allowing Putin to stay in power until 2036 come into force

Mass protests erupt in Belarus after the rigged presidential election