DEFENCE INTELLIGENCE AND SECURITY SERVICE UNDER THE MINISTRY OF NATIONAL DEFENCE

STATE SECURITY DEPARTMENT OF THE REPUBLIC OF LITHUANIA

2024

NATIONAL THREAT ASSESSMENT

DEFENCE
INTELLIGENCE AND
SECURITY SERVICE
UNDER THE MINISTRY
OF NATIONAL
DEFENCE

STATE SECURITY
DEPARTMENT OF
THE REPUBLIC OF
LITHUANIA

2024

NATIONAL THREAT ASSESSMENT

VILNIUS, 2024

CONTENTS

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 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 25 February 2024.

The table below outlines the language of probability and definition of terms used in this assessment:

< 25 %	25–50 %	50–75 %	> 75 %
UNLIKELY	POSSIBLE	LIKELY	HIGHLY LIKELY

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

Colonel Elegijus PAULAVIČIUS

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

Darius JAUNIŠKIS

Director of the State Security Department of the Republic of Lithuania

FOREWORD

Dear readers,

Lithuania's national security is affected by negative global security developments, which in recent years have been very significant. Russia's ongoing war against Ukraine, instability in the Middle East, hostile countries seeking to change the global security architecture – all these processes are highly dynamic. These dynamics also pose challenges for intelligence. With new crises reported almost daily, societies are in need of simple and quick answers. However, simple and quick answers are not always appropriate for explaining complex situations.

Intelligence is more often called upon to report bad news than good news. It must warn of threats and even worst-case scenarios because providing timely warning is one of its main tasks. However, the ability to communicate bad news to decision-makers is an advantage of living in a free and democratic country. In authoritarian regimes, the intelligence and security services often dare to provide their leaders with good news only, which leads to inadequate assessments of the situation, bad decisions,

and unjustified risks. The strength of intelligence is its access to non-public information, which allows it to provide a fuller picture of the situation and make assessments that are as close to reality as possible.

Lithuanian intelligence agencies provide information to the top state and military leaders, civil and military authorities so that they can use it in decision making. Along with these obligations there comes a great responsibility. In order to inform decision-makers in a timely manner, often there is no time to wait till all the data are collected and we have to provide the intelligence available at the moment, which is always accompanied by assessments of intelligence analysts. The language of probability or definition of terms is therefore unavoidable in intelligence work. Terms such as 'possible', 'highly likely' or 'in the medium term' are common in this publication, their definitions can be

found on the first pages of both this and previous editions of National Threat Assessment. These terms, which are also used by intelligence agencies in other Western countries, allow us to explain what is meant by one or another event, to interpret the fragmented intelligence obtained through various collection methods, and to provide an assessment of whether and when the situation will change.

We present our intelligence assessments to the public without revealing sensitive details, methods or secret sources of information in the ninth National Threat Assessment prepared by the Defence Intelligence and Security Service under the Ministry of National Defence and the State Security Department. We believe that the information on events and emerging threats affecting the security environment in Lithuania will be useful to readers at home and abroad.

SUMMARY

■ **Russia is allocating enormous resources to the war in Ukraine and shows no inclination to de-escalate the situation, even though it is failing to achieve its operational objectives**. At the same time, Russia is preparing for a long-term confrontation with NATO and has embarked on a major reform of its Armed Forces. Its full implementation will take from at least several years to a decade.

■ **Russia has financial, human, material, and technical resources to continue the war at a similar intensity in at least the near term**. The Russian economy is holding up better than expected thanks to high oil prices, state investment in the military industry, and the ability to circumvent sanctions. Military industry is becoming a driving force of Russia's economy at the expense of other sectors.

■ **The Kremlin attempts to portray itself as having universal support for its rule and policies**. However, the Wagner munity revealed that the regime was slow to react to the developing situation and that Russian society remained indifferent to the power struggle. The Russian presidential election remains a significant event to the Kremlin and serves as a tool to demonstrate the legitimacy of Putin’s power and the public approval of the regime’s policies. With a new mandate, the Kremlin is more likely to take unpopular decisions in the post-election period.

■ **Russia's foreign policy has been increasingly affected by its aggression towards Ukraine**. In its relations with the West, Russia's main objective is to undermine Western support for Ukraine by resorting to blackmail and threats. International isolation forces Russia to develop relations with the Global South, not only to secure alternative trade and logistics routes but also to form an anti-Western coalition with Russia as its leader.

■ **The Belarusian regime's threat perception is the driving force behind the intense activity of intelligence services against Lithuania**. Belarusian intelligence uses questionings of people who travel from Lithuania to Belarus and a growing Belarusian diaspora in Lithuania for its activities against Lithuania.

■ **Belarus' military potential is boosted by a significant increase in Russian arms support to Minsk**. The Kremlin is allowing Lukashenka to display a semblance of sovereignty and parity in decision-making. However, Russia seeks to maintain and increase its control over Minsk by building up a non-strategic nuclear weapons capability in Belarus and by establishing conditions for a sustained military presence through legal means.

■ **China intensifies intelligence activities against Lithuania from its territory**. Its intelligence services increasingly use social networks to establish and maintain contact with potential targets as well as cyber espionage against Lithuania. Chinese intelligence priorities are Lithuania's internal affairs, political divisions, and foreign policy. In the short term, Chinese intelligence services likely will seek to collect information on Lithuanian national elections, both presidential and parliamentary as well as the European Parliament election.

■ **The intensity of information attacks against Lithuania and neighbouring countrie has increased significantly**. These aggressive information operations are aimed at spreading fear among society members and disrupting work of state institutions. Russia's information policy is likely to intensify further, with new information attacks focused on elections, regional conflicts and support for Ukraine.

■ **The threat of Islamist terrorism in Europe is growing**. The Islamist propaganda disseminated by international terrorist organisations contributes to the increased probability of terrorist attacks. The main risk comes from lone radicalised individuals motivated not only by traditional Islamist propaganda narratives but also the deterioration of the situation in the Middle East.

AFP / Scanpix

RUSSIA

- In the near term, Russia will likely have the capacity to both continue the war in Ukraine and gradually expand its military capabilities westwards.
- Russia's military industry is able to adapt to sanctions, but deep structural weaknesses limit its expansion.
- The Kremlin attempts to portray itself as having universal support for its rule and policies. Institutions of power and propaganda remain loyal to the Kremlin.
- In its relations with the West, Russia's main objective is to undermine Western support for Ukraine, including through blackmail and threats. While by developing cooperation with the Global South, the Kremlin seeks to form an anti-Western coalition with Russia as its leader.

Russia allocates enormous resources to the war in Ukraine but still has the means to prepare itself for a protracted confrontation in the Baltic Sea region

Russia's war against Ukraine is gradually turning into a protracted conflict requiring increasing commitment of the Russian Armed Forces. To meet operational objectives and compensate for losses, Russia has sent troops and combat equipment *en masse* to Ukraine from units all over the country – even from the westernmost regions bordering NATO countries. Therefore, in the Baltic Sea region, Russia must increasingly use other components (air and naval) and nuclear capabilities to project its military potential and regional deterrence. In 2023, for example, Russia deployed Kalibr missile-capable ships on Lake Ladoga for combat duty for the first time, likely to signal its disapproval of Finnish NATO membership. In addition, Russian Tu-22M3 heavy bombers conducted five flights over the Baltic Sea in 2023, compared to none in 2022. In the summer of 2023, Vladimir Putin and Alexander Lukashenka also declared that Russian non-strategic nuclear weapons had been deployed in Belarus.

Tu-22M3 strategic bomber flights

Combat duty of Kalibr missile-capable small missile ships

A Tarantul-class small missile ship fires an anti-ship missile during an exercise
AP / Scanpix

The war in Ukraine affected even the previously untouched Russian A2/AD system in the Baltic Sea region. In late 2023, Russia moved part of its S-400 air defence system from Kaliningrad to Rostov-on-Don, likely to strengthen its air defence capability on the border with Ukraine.

With the vast majority of the Russian ground component deployed on the front line, the military training schedule in the Baltic Sea region had to be modified. The Zapad and Union Shield exercises did not take place. The latter was even publicly announced as having started at the end of September, but there were no signs of preparation or execution of the exercise on the ground. Russia therefore sought to compensate for the absence of these events by increasing the scale of the other two exercises dominated by air and naval components: the Baltic Fleet Operational Exercise and the Russian Navy's Ocean Shield exercise. It is likely that the war will continue to complicate the annual training schedule in 2024. Russia has announced a large-scale strategic exercise, Okean, in which air and naval forces less involved in the war against Ukraine will play a major role.

After more than two years of war against Ukraine, Russia shows no intention of de-escalating the situation. Even if it fails to achieve its operational objectives, the Kremlin is unlikely to abandon them. In the short term, Russia will continue to seek to extend its control to the administrative borders of the four occupied regions of Ukraine (Luhansk, Donetsk, Kherson, and Zaporizhzhya). In the long term, Russia's goals likely will remain unchanged: to completely undermine the Ukrainian statehood, to ensure its neutral status, and to destroy its military potential.

In 2023, Russia was able not only to reconstitute its military grouping in Ukraine, which had suffered heavy losses in the previous year, but also to strengthen it. On the battlefield, the Russian Armed Forces prioritise quantity over quality, attempting to crush the Ukrainian resistance through superiority in terms of troops, combat equipment, and ammunition. Moscow is able to evaluate the lessons learned and improve its combat effectiveness.

Russia has sufficient financial, human, material, and technical resources to continue fighting at a similar intensity, at least in the near term. Its chosen strategy is a war of attrition, based on the expectation of growing war-weariness in Western societies and governments and the diminishing will to fight among Ukrainians.

Despite the continued priority to the war against Ukraine, Russia has already begun the large-scale reform of its Armed Forces, announced in late 2022, and started to increase its military potential, including in the Baltic Sea region. Restructuring is a long-term project that will require effort and resources from several years to a decade. Russia is engaged in two parallel processes. It is both compensating for its losses in Ukraine and creating new capabilities for a long-term confrontation with the West. Changes in structure and subordination have already begun, including in the Kaliningrad region and Western Russia. The Western Military District is being divided into the Moscow and Leningrad Military Districts, which were merged in 2010. A new army corps is being formed in Karelia, while some brigades are being upgraded to divisions. These new formations can be created in a relatively short time, but building the necessary infrastructure and equipping the units with the required personnel and weaponry will take at least several years. All in all, the speed and scope of this reform will depend directly on the progress, duration, and outcome of the war in Ukraine.

Military industry becomes a driving force of the Russian economy

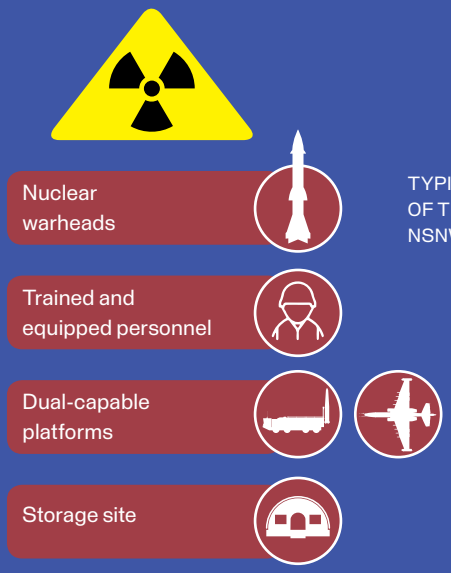
The war has cost Russia more than expected. The amount officially earmarked for Russia's military spending for the whole of 2023 was already exceeded in the first half of the year. Nevertheless, funding the Armed Forces remains the Kremlin's top priority.

Military allocations will make up at least a third of Russia's state budget in 2024 (more than 10 trillion roubles or 102 billion euros). The actual amount is certainly much higher, as it is supplemented by classified budget allocations. The war and the military industry are now driving the Russian economy, accumulating financial, material, and human resources at the expense of the other sectors of the economy.

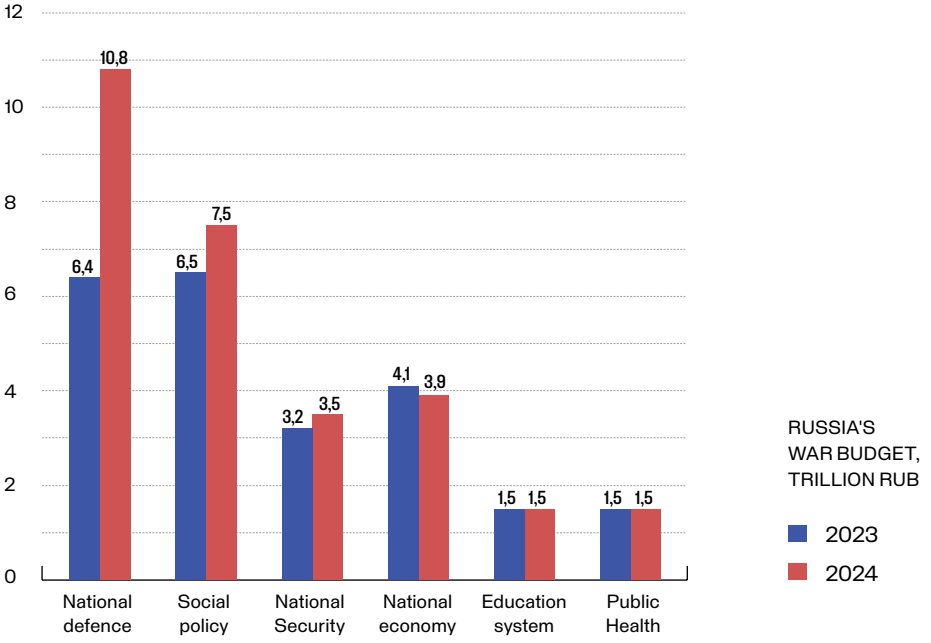
Russian nuclear capability in Belarus

The Russian nuclear arsenal consists of both strategic and non-strategic nuclear weapons (NSNW). The majority of strategic nuclear weapons are deployed in mobile missile systems or silos and form the Strategic Missile Forces. The remainder are deployed to be launched from strategic nuclear submarines or strategic bombers. NSNW can be launched from dual-capable platforms that can carry both conventional and nuclear warheads, thereby confusing the enemy in the event of an attack. NSNW play an important role in Russian military planning, providing a regional nuclear deterrent and compensating for a lack of conventional capabilities.

In 2023, Putin and Lukashenka announced that NSNW had been deployed on the territory of Belarus. Typically, the non-strategic nuclear capability is made up of several key elements: infrastructure for storing NSNW, dual-capable delivery systems, trained and certified personnel, and the nuclear warheads themselves. Over the past year, Belarus has made progress in many of these areas. The nuclear storage infrastructure has been renewed. The Belarusian Armed Forces have two potential nuclear delivery means – Su-25 attack aircraft based at the Lida airbase near the Lithuanian border and mobile Iskander-M missile systems at Asipovichy. Belarusian military personnel are being trained to operate with NSNW. All these elements suggest that a credible nuclear capability is being built in Belarus. In any case, full control of NSNW will remain in Russian hands. Russia will use Belarusian territory and personnel but will retain the right to decide whether and how NSNW will be used. The deployment of NSNW in Belarus will only deepen the ties between the two countries and encourage Moscow to maintain control over Minsk at all costs.



Russia's economy is in better shape than expected due to high oil prices, government spending, and the ability to circumvent sanctions. Russia has not exhausted its resources or the potential of its public and private sectors. Nor is it completely isolated. As a result, it is able to meet its growing expenses and does not feel any critical pressure to change its political course.



After the large-scale invasion of Ukraine in 2022, Russia's military industry grew mainly because of the accumulated reserves and the government's focus on improving and monitoring production processes. The ability to import sanctioned foreign components and equipment through third countries and various schemes has mitigated the impact of international legal restrictions on Russia.

The circle of Russian supporters remains similar. China is the largest supplier of microchips to Russia, and the yuan has

The international sanctions regime is a significant constraint on Russia's ambitions to develop its military industry
IMAGO / Scanpix

become the main currency for Russia's international transactions. Russia also imports electronics via countries of Central Asia and the South Caucasus. However, large companies from these countries avoid direct cooperation with Russia for fear of sanctions. It is usually intermediaries and smaller private companies that carry out these activities.

Only two countries, Iran and North Korea, which are themselves under sanctions, openly supply Russia with military goods. They provide Russia with the weapons and ammunition it needs to continue the war. Drones from Iran have been instrumental in depleting Ukraine's air defences, allowing Russia to save its own missile arsenal. In 2023, North Korea began large-scale deliveries of ammunition, signalling Russia's willingness to maintain the intensity of the fighting. The shells are of low quality but sufficient for Russia's war of attrition.

However, in order to continue the war while rebuilding its military capabilities, Russia will face structural problems that are likely to deepen over time and as the war drags on. The current growth of Russia's military industry is driven by short-term factors and has its limits.

Russia's long-term negative demographic trends, exacerbated by the war, are leading to a shortage of skilled labour. High wages and protection from mobilisation are short-term solutions to attract workers, and it aggravates labour shortages in other sectors of the economy.

Industrial development is also constrained by Russia's reliance on foreign technology, including its critical dependence on manufacturing tools. Circumvention of sanctions does not guarantee Russia a sustainable and adequate supply of electronics and equipment. New sanctions and restrictions force Russia to change acquisition schemes, raise the cost of these components, and increase Russia's dependence on its partners.

Russia expects such dependences to be temporary. The Kremlin's import substitution efforts have borne fruit in some areas (such as UAV production) thanks to clearer priorities and targeted funding.

However, deep structural problems would hamper the modernisation of production and Russia's ability to establish significant technological sovereignty. As a result, the Kremlin will need to further strengthen its control over the economy in order to direct resources for solving current problems. However, Russia is likely to be able to build up its military capabilities and finance the war against Ukraine in the short term.

Russian intelligence services – the Foreign Intelligence Service (SVR), the Main Directorate of the General Staff of the Russian Armed Forces (GRU), and the Federal Security Service (FSB) – are involved in organising the import of sanctioned goods and equipment into Russia.

Companies operating in Russia's strategic industries cooperate with intelligence services and provide them with 'shopping lists' containing Western high-tech equipment or components that Russian intelligence services are supposed to acquire. The procurement of sanctioned equipment and components is organised by Russian intelligence officers under diplomatic cover or by Russian and Western citizens cooperating with Russian intelligence. Russian intelligence services constantly seek for and exploit loopholes in sanctions control procedures as well as organise procurement via third countries.

Russian strategic industries will face difficulties in the near term as a result of the sanctions. It is therefore highly likely that Russian intelligence services will increase their efforts to procure and supply the necessary equipment, production or technological innovation to Russia. It is also highly likely that to achieve this goal they will use supply chains, logistics infrastructure or individuals seeking to profit from the sanctions evasion.

Wagner crisis has pushed Russia towards Volunteer Corps as a new model of military service

Russia has been using private military companies (PMCs) as a military tool abroad for a decade (first in Ukraine, then in Syria, and later in Africa). Russia uses PMCs to deny its involvement and responsibility and to speed up decision-making. However, the independence of PMCs is only part of their image. Russian intelligence services informally coordinate their operations, while funding comes from Kremlin-linked actors and through public procurement systems.

Since February 2022, mercenaries have been massively involved in military actions in Ukraine. Their illegal status under Russian law raised complex issues of subordination and coordination with the Russian Armed Forces. Therefore, in November 2022, a special legal amendment granted the Russian Ministry of Defence the right to use subordinate 'volunteer formations' in its operations. Russia's largest PMC, Wagner, had tried to maintain its independence on the front line, but when the conflict resulted in an armed mutiny, it became a final argument for the Kremlin to tighten control over its shadow army.

Since 1 July 2023, all PMCs wishing to take part in military operations in Ukraine have had to sign a contract with the Russian Ministry of Defence as volunteers. The Russian Armed Forces now use Volunteer Corps, made up of mercenaries, Cossacks, active reserve soldiers, and volunteer units formed by regional authorities and state enterprises, to fill gaps on the Ukrainian front. While mercenary activities remain illegal under Russian law, conditions have been created to employ them in war with sufficient control.

The Russian regime, reluctant to announce a new wave of mobilisation, is trying to convince its citizens to join the war voluntarily. It has set itself the goal of recruiting more than 400,000 new soldiers in 2023 and is continuing the recruitment this year. In addition to the usual contracts, volunteer formations have become another way of recruiting people for war.

The new model of volunteer corps is also being implemented outside Russia. It enables Russia to maintain influence in crisis regions without withdrawing its troops from Ukraine. In the near future, destabilising activities of such expeditionary units will be increasingly visible around the world, although in 2024 Russia will focus mainly on Africa.

Putin's election as an aspiration for legitimisation, which impacts political agenda

The Russian presidential election remains a significant event in the country's political landscape. It serves as a tool to demonstrate the legitimacy of Putin's power and the public approval of the Kremlin's policies. Moreover, the election is instrumental in dissemination the regime's propaganda. In preparation for the 2024 presidential election, the regime sought to ensure that the support for the Russian leader had not diminished since the last election, and that at least half of the eligible population would vote for Putin.

THE RESULTS OF RUSSIAN PRESIDENTIAL ELECTION

- Columns indicate voter turnout
- The percentage of votes casted for the winner
- The percentage of all eligible voters who casted their votes for the winner of the election
- Regime's goals for the 2024 presidential election

The manipulation of the electoral process has been perfected under the Putin rule. Election authorities, with the Kremlin's approval, have marginalised the non-systemic opposition, denied them access to the election enforced the dominance of pro-regime candidates in the media, pressured state officials, employees of

state-owned companies or companies owned by loyal oligarchs, facilitated non-transparent Internet voting and gerrymandering. The Russian Presidential Administration, together with other institutions, imitate democratic procedures and seek to demonstrate that the election is transparent and its results are legitimate. However, if the desired election results cannot be achieved through political technologies and procedural manipulations, repression of society and control of the media, both of which have intensified over several years, provide the regime with additional opportunities to falsify the results as it sees fit.

One of the Kremlin's priorities has been to ensure that Putin's approval rating among the population of the newly occupied territories of Ukraine is higher than Russia's average. These election results would be used by the regime to justify Russia's invasion of Ukraine and legitimise the annexation of the Ukrainian territories.

Putin's election campaign has been based on ideology, it emphasises Russia's uniqueness, sovereignty, the need to preserve traditional values and an inevitable confrontation with the West. Since the non-systemic opposition has been neutralised, the Kremlin, after the failed Yevgeny Prigozhin's mutiny, pays more attention to the so-called ultra-patriots by preventing them from criticising the Kremlin's regime. Therefore, war propaganda has been an essential element of the election campaign, as the Kremlin wants to appear more patriotic than the ultra-patriots.

The regime has been also determined to show that the war has little impact on people's daily lives. In the run-up to the the election, the Kremlin has avoided any unpopular decisions that could have increased social discontent (e.g. announcing a second wave of mobilisation or cutting social spending). With a new mandate, the Kremlin is more likely to take unpopular decisions in the post-election period to address problems related to the situation on the frontline or the country's economy.

Unexpected challenge of Wagner mutiny the regime managed to overcome

The Kremlin attempts to portray itself as having universal support for its rule and policies, but Prigozhin's mutiny revealed a potential fragility of the authoritarian regime as well as Russian society's attitude towards it.

THE WAGNER MUTINY CAME AS A SURPRISE TO THE KREMLIN. Wagner mercenaries entered Rostov-on-Don without resistance and were even on the move towards Moscow. At the beginning of the mutiny, the regime propaganda and prominent regime figures refrained from making public statements until Putin publicly named Prigozhin a rebel and expressed his determination to put an end to the mutiny. The reluctance to denounce mutineers' actions before Putin did it was likely due to the fear of misinterpreting the actions of Prigozhin, who before the mutiny had been an integral part of the regime and the main symbol of Russia's aggression against Ukraine.

INSTITUTIONS OF POWER REMAINED LOYAL TO THE KREMLIN. It is likely that this was one of the reasons for the failure of Prigozhin's mutiny. The propaganda apparatus also remained loyal, and after the revolt had failed, it tried to discredit Prigozhin without inciting hostility towards Wagner. The Kremlin's position that it is important not to discredit the aggression against Ukraine in spite of the actions of those who took part in the mutiny but stood against the regime, is an indication that the regime is becoming a hostage of its own propaganda.

THE MUTINY CONTRADICTS THE REGIME'S NARRATIVE OF THE UNIVERSAL SUPPORT FOR THE PRESIDENT. Society remained indifferent to the unfolding events. Neither the mutiny nor Prigozhin's death has led to an increase in civic activity or encouraged ordinary citizens to take action for or against the government. In the aftermath of the mutiny, Putin himself took part in several public appearances aimed at demonstrating his 'closeness to the people', but these actions have not culminated in any substantial effort by the regime to rally public support for the Kremlin.

The Kremlin remains determined to continue its aggressive policies and tighten its control over society. Public dissatisfaction with the regime's policies is unlikely to threaten its stability in the short term. The mutiny provided an opportunity for the Russian National Guard to demand more resources. As a result, the Kremlin is now likely to increase its readiness to respond to threats of coups or mutinies. However, the crisis has exposed the fact that the centralised control system of the authoritarian regime is incapable of responding quickly to the changing situation and that unexpected challenges increase the likelihood of instability.

Ideology-driven Russia's foreign policy fosters global instability

Russia's foreign policy has been increasingly affected by its aggression towards Ukraine. Iran and North Korea have become Russia's closest partners directly supporting its military efforts. In its relations with the West, Russia's main objective is to undermine Western support for Ukraine. Developing cooperation with the Global South is essential for Russia in order to secure alternative trade and logistics routes as well as to secure export markets for energy resources and other goods.

Although the Russian regime frequently mentions the necessity of constructing a multipolar world order, the only purpose of this narrative is to form an anti-Western coalition, which would comprise primarily of the Global South states, with Russia leading the coalition.

The goal of building such a coalition is declared in the new Russia's Foreign Policy Concept, adopted in 2023. This document outlines Russia's uniqueness, a 'state-civilisation', and its ambition to create a new world order. It begins with the narrative that Western neo-colonialism supposedly ensures its hegemony. The central goals of Russia's foreign policy are defined as the dominance in the region of the Commonwealth of Independent States (CIS) and strategic cooperation with China and India. The concept also lists in detail foreign policy objectives towards Muslim countries, Africa, and Latin America. The United States and Europe are described as adversaries whose influence shall be limited.

Russia's stance on the Israel-Hamas and Armenia-Azerbaijan conflicts is a good example of how opportunistically Russia conducts its foreign policy. Russia's support for the authoritarian regimes and attempts to consolidate its influence in Africa, including with the help of PMCs, directly contribute to a worsening of the security and political situation in the Global South.

Russia is increasingly resorting to blackmail and threats, including the use of nuclear rhetoric, to force the West to scale back its support for Ukraine. The deployment of non-strategic nuclear weapons in Belarus, the decision to withdraw the ratification of the Comprehensive Nuclear-Test-Ban Treaty, and public reflections by some Russian figures, such as Sergey Karaganov, on the benefits of nuclear

proliferation reinforce this rhetoric. In effect, Russia is trying to demonstrate its determination to escalate the situation further and to assert that the West shall change its policy towards Russia if it is interested in a constructive relationship.

The aggression against Ukraine is forcing the Kremlin's regime to consider increasingly radical decisions that could help Russia overcome its international isolation. However, countries that have not supported sanctions against Russia, including China, are using economic cooperation with Russia primarily for their own benefit. This is despite the fact that both Russia and China are interested in limiting the Western influence. The exploitative nature of such relationships hinders the growth of Russia's international influence in the long term – Russia lacks economic and military resources to consolidate its power status.

Protracted war makes Russian intelligence officials question the validity and legitimacy of their activities

Russia's full-scale invasion in Ukraine is having a negative impact on the malicious activities of some Russian intelligence services. Since 2023, Russian intelligence officers have been increasingly dissatisfied with the decisions of the Russian authorities and reluctant to contribute to Russia's aggressive policies. This not only affects the quality of their duties but also encourages them to assess the possibility of cooperation with Western authorities. Hasty, ill-considered and sometimes unprofessional decisions made in the Russian services lead to mistakes and unassessed risks that not only undermine the efficiency and results of activities but also increase the number of identified cases of malicious activity.

Attempts of intelligence services to recruit Lithuanian citizens travelling to Russia are becoming less scrupulous. Russian intelligence officers are cooperating with the Russian Migration Service and conducting interviews with foreigners at the border to identify suitable targets for recruitment. However, recently there has been an increasing number of cases

where proposals for cooperation were made without a proper screening of the candidates or assessment of foreigners' willingness to cooperate. Recruiting officers do not consider either that the pretext used for blackmail – administrative offences committed on Russian territory (traffic accidents or artificial situations requiring involvement of law enforcement) – often does not change the beliefs of the foreigners they are attempting to recruit or outweigh the perceived harm of cooperating with authorities of hostile countries. Furthermore, there were attempts to recruit not only those travelling to Russia but also those in their immediate environment. This pattern of recruitment leads to even more people exposed to recruitment attempts and willing to report it to Lithuanian intelligence services.

It is highly likely that the motivation of Russian intelligence officers will further weaken as the Russian military conflict in Ukraine continues. There will be more cases of officials trying to demonstrate their perceived importance and please their superiors by doing seemingly useful but inefficient and unprofessional work. One of their goals is likely to avoid personal involvement in Russia's war in Ukraine. Their negligence will lead to proliferation of mistakes that will facilitate the work of Lithuanian counter-intelligence authorities in uncovering those involved in criminal activities and revealing methods used by Russia.

Locations of a meeting between Russian intelligence officers and agents in Kaliningrad (Turist Hotel and Zoo)

Russian and Belarusian intelligence agencies are aggressively seizing the opportunity to recruit foreigners in Russia and Belarus. They are aided by political leadership of the countries in passing laws to facilitate these procedures.

In autumn 2023, the Belarusian authorities started to discuss legislative changes that would require Belarusian residents to inform the Ministry of Internal Affairs if they rented premises to foreigners. This change will mean that the Belarusian authorities will be informed about the presence of any foreigners in Belarus, even those who have not been obliged to register so far. As a result, the authorities will be able to collect more data on the residing foreigners.

Russia is considering obliging all foreigners to sign a 'loyalty contract'. Once the proposal enters into force, foreign nationals will have to sign a special document pledging not to 'discredit' or interfere with the Russian Federation's public policies, institutions or officials. The signing of such an agreement is likely to lead to prosecution of foreigners for disseminating information that is not in favour of the Russian authorities. It is likely that such a mandate will be used as a pretext for stricter restrictions on the rights of foreign citizens in Russia as well as for legal persecution and, consequently, for possible recruitment.

In the second half of 2023, several Lithuanian citizens were detained in Lithuania on suspicion of cooperating with Belarusian intelligence authorities. They are suspected under Article 119(2) of the Criminal Code of the Republic of Lithuania (espionage). The detainees were almost certainly carrying out tasks for Belarusian intelligence and were collecting and passing on information to the client for a fee. None of the persons in question had a clearance to handle classified information, worked with such information or had a possibility to collect it. Although the information on the country's critical infrastructure and military facilities these persons collected and communicated was unclassified, these non-public data non-public data could be used by the Belarusian non-democratic regime to plan activities against Lithuania. It is almost certain that the information the citizens of the Republic of Lithuania passed on to foreign intelligence agencies is necessary for the Armed Forces of both Belarus and Russia to prepare plans for potential military aggression against neighbouring countries.

BELARUS

- Belarusian intelligence services conduct intensive and aggressive activities against Lithuania.

- Russia publicly supports the alleged Lukashenka's sovereignty in military-security matters while at the same time creating a legal basis for a long-term military presence in Belarus.

- In response to the regional security situation, Lukashenka has been building up his forces, creating new units, and receiving unprecedented armaments support from Russia.

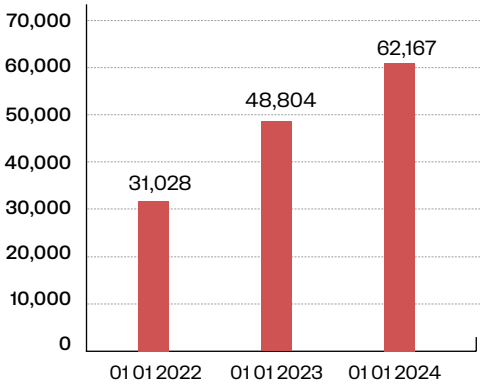
- The Belarusian regime is maintaining control over the country and keeping its economy stable. The Lukashenka regime is currently in the final stages of the political system reform; it seeks to create an illusion that Belarusian domestic political scene is undergoing a positive change.

Belarusian regime's threat perception is the driving force behind the intense activity of intelligence services against Lithuania

The Belarusian regime perceives Western support for the Belarusian democratic opposition and Belarusians fighting on the side of Ukraine as the main threats to its security. To counter these threats and safeguard the ruling regime, Belarusian intelligence services have expanded their intelligence operations abroad and strengthened domestic counter-intelligence. Belarusian intelligence has been focusing on the Belarusian opposition based in Lithuania as well as on a growing community of Belarusians. As a result, Lithuania has become one of the main targets for Belarusian intelligence services.

The Belarusian diaspora in Lithuania consists of over 62,000 Belarusian citizens and grows by about 15,500 people annually. It includes members of the political opposition and non-governmental organisations, independent journalists who fled the country because of the regime's persecution after the rigged 2020 presidential election as well as of economic migrants.

A growing Belarusian diaspora in Lithuania provides an opportunity for Belarusian intelligence services to find targets for recruitment. Contacts between Belaru-



DYNAMICS OF THE BELARUSIAN DIASPORA IN LITHUANIA

(Source: Migration Department of Lithuania)

sian intelligence and some members of the Belarusian diaspora pose a significant threat to Lithuanian national security, particularly when maintained after their arrival in Lithuania. Belarusian intelligence services exploit former employees of Belarusian state institutions who currently reside in Lithuania. This activity is made possible due to the system of agent recruitment in Belarus that the country's intelligence services run in state institutions, strategically important entities, and the armed forces. Belarusian intelligence services have recently begun to establish and re-establish contacts with members of the Belarusian diaspora and recruit new intelligence assets using modern remote communication methods.

In addition to counter-intelligence threats, the growth of the Belarusian diaspora in Lithuania has brought other challenges. Some members of the diaspora promote radical political ideologies, such as Litvinism, a radical branch of Belarusian chauvinism, which has recently attracted attention in Lithuania. Litvinism denies the Baltic origin of the dukes of the Grand Duchy of Lithuania and questions the rights of the Republic of Lithuania to the Vilnius region. Some Lithuanian-based adherents of Litvinism actively promote their ideological views on social media. A widespread dissemination of such views among the Belarusian diaspora has a negative impact on the integration of Belarusians into society and could lead to an increase in ethnic tensions. The Belarusian regime conducts information attacks themed around Litvinism to incite confrontation between Belarusians living in Lithuania and Lithuanian society.

Some members of the Belarusian diaspora also support far-right ideologies. In late 2023, the Belarusian cell of the international right-wing extremist network 'Active Club' was established in Lithuania. 'Active Club' is an extremist movement inspired by the American far-right activist Robert Rundo. Its followers combine promotion of right-wing extremist ideologies and the dissemination of propaganda with martial arts and other physical activities.

Belarusian intelligence services use members of the Belarusian diaspora to collect information on Lithuanian institutions as well as on the Belarusian democratic opposition and the diaspora itself.

According to available information, Belarusian intelligence intensively uses questionings of people who travel from Lithuania to Belarus and collects information for its activities against Lithuania. These questionings have peaked in 2023 and while their primary purpose is ostensibly to prevent threats to the Belarusian regime, they are also used to gather intelligence and identify individuals with a potential for intelligence activities in Lithuania.

Belarusian intelligence officers inspect mobile devices and personal computers of individuals seeking to enter Belarus, check their contact lists, social media accounts, and photographs for any relevant information. While questioning and performing checks, Belarusian intelligence services collect information on the travellers' purpose of visit to Belarus, their political views, employment. They also investigate whether individuals crossing the border have any links to the State Border Guard Service of Lithuania, law enforcement agencies, Lithuanian intelligence, or the military. Belarusian intelligence services attempt to identify current and former employees of state and municipal institutions, the judiciary, law enforcement agencies, and the Lithuanian armed forces, as well as businesspeople, employees of strategic companies, journalists, and individuals involved in illegal activities. Belarusian intelligence services seek to recruit individuals who have a potential to provide relevant intelligence or perform other tasks. Belarusian intelligence officers may use psychological pressure and blackmail to coerce individuals to cooperate based on various traffic accidents, violations of law, visa regulations, or border crossing procedures.

We assess that the Belarusian regime's perception that Lithuania and other neighbouring countries pose a threat to its stability is the driving factor behind the increased activity of Belarusian intelligence against Lithuania. It is highly likely that Belarusian intelligence services will continue to target Lithuania, its citizens in Belarus, and the Belarusian diaspora in Lithuania in the near term. Belarusian intelligence services are likely to use members of the growing Belarusian diaspora to gather intelligence in Lithuania. Additionally, they will continue to target individuals travelling to Belarus for personal, tourist or other purposes in order to gather information and identify potential candidates for recruitment.

Sign at Lithuania's border with Belarus warning travellers of the dangers of visiting Belarus
EPA / STRINGER / Scanpix

Recently, Belarusian intelligence services started to target the staff of the Lithuanian diplomatic mission in Belarus. Belarusian intelligence observes the Lithuanian Embassy personnel and collects information about their relations, habits or anything that could compromise them. The collected information or administrative measures are used to intimidate the employees. By carrying out such activities, Belarusian intelligence services aim to recruit Lithuanian diplomatic mission employees and force them to act against Lithuania's national security interests.

Calm facade of Belarus conceals political repression

As Russia's aggression against Ukraine enters its third year, the Belarusian regime is maintaining control over the country and keeping its economy stable. Lukashenka's efforts to mitigate the impact of international sanctions imposed on Belarus have been largely facilitated by the financial and economic aid from the Kremlin.

The Lukashenka regime is currently in the final stages of the political system reform. On 25 February 2024, the Single Voting Day, new parliament members and local representatives were elected. In the coming few months, a new institution, the All Belarusian People's Assembly, will be established. Following the ban and dissolution of almost all political parties in 2023, the Belarusian regime permitted only three pro-government political parties to continue their activities after the re-registration: the Belarusian Communist Party, the Liberal Democratic Party, and the Republican Party of Labour and Justice. In addition, a new party, Belaya Rus, was formed, which likely will become the main pro-regime party in Belarus. All the four parties likely will be allowed to oppose each other, thus creating an illusion that Belarusian domestic political scene is undergoing a positive change. In reality, all opposition political parties have been dissolved and their members persecuted or imprisoned.

Repression of Belarusian citizens continues. Human rights organizations have recorded approximately 1,500 political prisoners in Belarus, including journalists, businesspeople, supporters of former presidential candidates, and participants of the 2020 protests against

the Lukashenka regime. The Belarusian regime continues to persecute Belarusian citizens who participated in the 2020 protests or who express any form of opposition to the regime. Even sharing an opinion critical of the regime on social media is enough to trigger the regime's reprisals.

Political prisoners are mistreated and tortured at imprisonment facilities. Human rights centre Viasna has obtained a testimony of one of the political prisoners sentenced to two and a half years in prison for participating in the 2020 protests and placed in the penal colony No. 17 in Shkloŭ. According to the former prisoner, he spent three weeks in a solitary confinement cell for a misdemeanour during his incarceration. He was forced to sleep on a wooden bed without any bedding. The temperature in the cell was maintained at a maximum of 10 degrees Celsius. In addition, the cell window remained open from 7 am to 2 pm, even when the outside temperature dropped below 0 degrees Celsius. During his time in the solitary confinement cell, the prisoner was denied the ability to shower and was prohibited from sleeping, reading or writing during the day. The former prisoner lost 17 kilograms of his weight during the imprisonment due to insufficient food.

The information on the condition of prominent opposition activists, including former presidential candidates Viktar Babaryka, Syarhei Tsikhanouski, Mikalai Statkevich, and Maryia Kalesnikava, is not available. No one is allowed to visit them, and they are denied the right to contact their families or lawyers.

Lukashenka builds up Armed Forces in response to regional security situation

In recent years, the Lukashenka regime has paid more attention to the mobilisation and combat readiness of the Armed Forces, learning Russia's lessons from the war against Ukraine. In 2023, Belarus revised the procedures for calling up reservists; the recently amended laws allow for accelerated mobilisation of

reservists and an increase in the number of reservists. Since the end of 2022, Belarus has intensified the combat readiness training of manoeuvre units. In 2023, the Armed Forces tested the transition of a mechanised brigade to a wartime establishment. In addition, Wagner mercenaries provided training and passed on the latest combat experience to the Armed Forces and the Ministry of Internal Affairs.

Belarus has also increased its military presence towards Ukraine. In addition to the manoeuvre units that have been patrolling the Ukrainian border since spring 2022, a new regiment equipped with S-300 surface-to-air missile complexes was formed in Luninets in early 2023. It is planned to establish a new garrison with training facilities in the Gomel region.

The delivery of Iskanders and S-400 systems to the Belarusian Armed Forces likely meets Russian operational needs
Belarus Ministry of Defence

RUSSIAN MILITARY PRESENCE IN BELARUS AND REINFORCEMENT OF THE BORDER WITH UKRAINE

Russian ground forces reconstituted in Belarus from October 2022 to July 2023

In July 2022, bulk of Wagner mercenaries moved to Belarus

Russian combat aircraft

Russian surface-to-air missile units

New surface-to-air missile regiment was established at the beginning of 2023

Since spring 2022, the border with Ukraine has been reinforced with Belarus manoeuvre missile units

In 2023, Belarus has acquired a significant amount of modern combat equipment from Russia. The Iskander operational-tactical missile complex was delivered to Belarus. Its guided missiles have a range of 500 km and can carry both conventional and nuclear warheads. The Special Operations Forces received a battalion set of BTR-82A armoured personnel carriers. Belarus strengthened its Air and Air Defence Forces with new S-400 surface-to-air missile systems and Mi-35M attack helicopters. The growing combat and mobilisation readiness of the Belarusian Armed Forces as well as the significant assistance provided to Belarus by Russia in the form of military equipment are increasing the country's military potential.

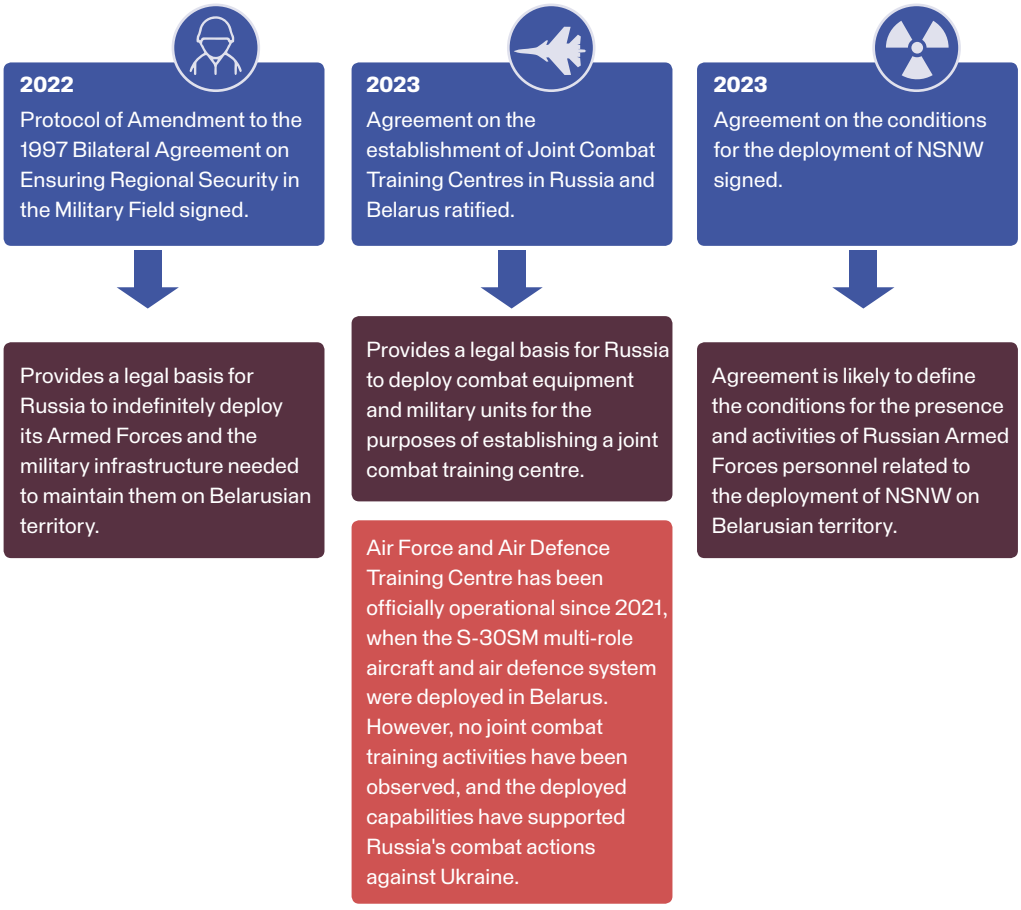
Russia allows Minsk to demonstrate its sovereignty on military-security issues but pursues its military policy in Belarus

By supporting Russia's military-security interests, Lukashenka seeks to project an image of a decision-maker on an equal footing with the Kremlin. However, it is very likely that Minsk's equivalence is often only imaginary. Belarus' public communication is often at odds with Russia's actual steps. However, Russia itself increases Lukashenka's political legitimacy by backing up his claims of joint decision-making.

For example, it was publicly announced that the Russian military grouping deployed in Belarus prior to the Russian invasion of Ukraine was supposedly there because of military training organised at Lukashenka's suggestion in order to strengthen Belarusian security. When Russia started sending mobilised troops to Belarus for training in autumn of 2022, Lukashenka and Putin presented this as the activation of a Regional Military Grouping to protect the borders of the Union State, but the observed joint activity with the Belarusian Armed Forces was highly symbolic. In July 2023, when the Russian ground forces contingent left Belarus, the regime continued to emphasise external threats and announced it was looking forward to a new rotation of Russian troops. However, in the second half of

the year, no more Russian ground troops arrived in Belarus. This case shows that in some cases Belarus is forced to interpret Russia's actions on its territory, probably without always knowing exactly what Russia intends. The deployment of Russian NSNW in Belarus is also presented by both sides as Lukashenka's initiative, but it is very likely that this process is primarily a matter of Russia's interests being served by taking advantage of Minsk's dependence.

The defence ministers of Russia and Belarus sign an agreement to establish conditions for the deployment of NSNW
EPA / Scanpix



AGREEMENTS SIGNED IN RECENT YEARS LEGALISING RUSSIA'S MILITARY PRESENCE IN BELARUS

CHINA

- China intensifies intelligence activities against Lithuania. Its intelligence services increasingly use social networks to establish and maintain contact with potential targets as well as cyber espionage against Lithuania.

- Chinese intelligence priorities are Lithuania's internal affairs, political divisions, and foreign policy. In the short term, Chinese intelligence services likely will seek to collect information on Lithuanian national elections, both presidential and parliamentary as well as the European Parliament election.

- The Chinese Communist Party (CCP) exploits a wide intelligence network, including government and private entities, universities, and NGOs to reach its strategic goals.

China intensifies intelligence activities against Lithuania from its territory

The significantly reduced capabilities of the Chinese diplomatic mission and unfavourable counter-intelligence regime in Lithuania have restricted the ability of Chinese intelligence services to collect information in Lithuania or directly influence the country's socio-political affairs. As a result, Chinese intelligence services are concentrating on developing an agency in Lithuania and collecting intelligence from Chinese territory.

Chinese intelligence services actively use the social network Linkedin for targeting, as its users publicly disclose a significant amount of personal information
AFP / Scanpix

Similarly to other Western countries, one of the most common methods used by Chinese intelligence services to establish and maintain contact with potential targets is via social networks. Chinese intelligence uses social networks to identify persons of interest who fit their target profile. These individuals may have direct access to sensitive information or a wide network of contacts, including officials, politicians, journalists, businesspeople, scientists who can be used as intermediaries in intelligence operations. Chinese intelligence officers usually use the cover of representatives of various companies or think tanks when approaching targets, offering financial incentives for information. Targets are typically invited to travel to China, where they receive their payment and new intelligence assignments.

Chinese intelligence services have also increased cyber espionage against Lithuania. Cyber actors affiliated with China regularly conduct vulnerability scans of networks of Lithuanian government institutions with the aim of penetrating their networks and exfiltrating data.

In recent years, intelligence requirements of Chinese intelligence services for information related to Lithuania have changed. Previously, China was mostly interested in information about the 'five poisons' (Taiwan, Hong Kong, Tibet, Xinjiang, and Falun Gong) as well as Lithuania's role in the EU and NATO. Currently, Chinese intelligence priorities have shifted towards Lithuania's internal affairs, political divisions, and foreign policy. In the short term, Chinese intelligence services likely will seek to collect information on Lithuanian national elections, both presidential and parliamentary as well as the European Parliament election.

We assess that the risk of Chinese intelligence services targeting Lithuanian citizens travelling to China has increased since China lifted the pandemic restrictions and allowed travel for business, academic, and cultural exchange purposes. Chinese intelligence is likely to approach Lithuanian citizens during their visits to third countries, particularly in Southeast Asia, where there is no strict counter-intelligence regime, thus creating favourable conditions for Chinese intelligence to operate.

China collects information and conducts influence activities in foreign countries using the whole-of-society approach

The Chinese Communist Party (CCP) exploits a wide intelligence network to reach its strategic goals. Besides traditional intelligence services, the network includes the CCP bodies, Chinese government and private entities, universities, and NGOs. The CCP's intelligence requirements encompass information about foreign countries' scientific and technological potential, economic situation, foreign and defence policies, socio-political developments, and methods of influencing domestic politics. In order to collect intelligence, the regime has created a complex intelligence system which extends throughout entire Chinese society (please see the figure on page 50-51).

The Chinese intelligence system consists of three traditional intelligence services: the Ministry of State Security (国家安全部, MSS), responsible for civilian intelligence; the Ministry of Public Security (公安部, MPS), responsible for civilian counter-intelligence and some intelligence activities; and the Military Intelligence Directorate (军事情报局, MID), responsible for military intelligence and counter-intelligence.

Although hierarchically all of these services are under the jurisdiction of the government (MSS and MPS) or the People's Liberation Army (MID), in reality, all three are directly coordinated and tasked by the highest CCP authorities.

MSS and MID carry out political, economic, and military intelligence in foreign countries by exploiting networks of agents who have access to classified or other sensitive information. Intelligence services establish and develop their contacts through social networks such as *Linkedin*; officers use both official and non-official cover. Chinese intelligence services typically recruit their agents and provide payment for their services in China. In addition, loosely interpreted national security legislation creates conditions that allow Chinese intelligence services to force individuals to cooperate by using threats, compromising information, and blackmail. Intelligence services also use SIGINT and CYBERINT to penetrate foreign government institutions, private companies and critical infrastructure networks and intercept their information.

Over the past decade, the CCP has been consistently developing the legislation regulating the activities of Chinese intelligence services. The CCP aims to broaden the concept of national security, to further expand the mandate of intelligence services, to ensure effective coordination, and develop an intelligence support system that engages the whole of Chinese society. The legislation governing the activities of intelligence services and China's foreign policy currently states that:

- Chinese citizens, government institutions, political parties, enterprises and organisations are obliged to safeguard the country's sovereignty, dignity, honour, and interests at home and abroad.
- Chinese citizens and organisations are obliged to provide information and other assistance to Chinese intelligence services in order to protect China's national security interests.
- Chinese citizens travelling abroad for study, work or internship are required to respond to threats to China's national security. They are briefed before leaving China in accordance with the counter-intelligence risk prevention programme and debriefed by counter-intelligence officers upon their return.
- Chinese business companies must ensure that Chinese intelligence services have access to their documents, computers, data storage, information systems, and physical infrastructure.
- Telecommunications companies and Internet service providers based in China are required to store their data on Chinese territory and to ensure that Chinese government agencies have access to it for inspections.
- Chinese institutions have the right to take action against foreign entities in China if they determine that the entity is involved in the implementation of sanctions against China.
- Chinese intelligence services have the right to detain foreign citizens in China if they determine that the foreign citizen possesses information relevant to the national security. Publicly available data, such as Internet search history, official statistics, maps and photographs may be considered sensitive information by Chinese intelligence services.

As a counter-intelligence agency, the MPS differs from the MSS and MID in its *modus operandi*. With the Chinese police forces at its disposal to ensure the counter-intelligence regime, the MPS collects information on the opponents of the CCP, supporters of the autonomy for Tibet, Hong Kong and Taiwan, foreign citizens residing in China, and the activities of foreign companies. MPS officers are often sent abroad under diplomatic cover or on a temporary basis. Once overseas, the main purpose of the MPS is to monitor and intimidate Chinese dissidents and opponents of the CCP in order to force them to return to China, where they would face criminal prosecution. These MPS's activities are also known as 'Operation Fox Hunt' (猎狐行动).

Beijing is focused not only on expanding China's influence but also on ensuring that the CCP is recognised internationally as legitimate, that its policies and interests are supported by foreign countries, and that its ideology is backed by the Chinese diaspora. To pursue these goals, the CCP has established two entities within the Party: the International Department of the Communist Party of China (中共中央对外联络部, IDCPC) and the United Front Work Department (统一战线工作部, UFWD). These are structural parts of the CCP, but their activities have many characteristics usually attributed to intelligence services.

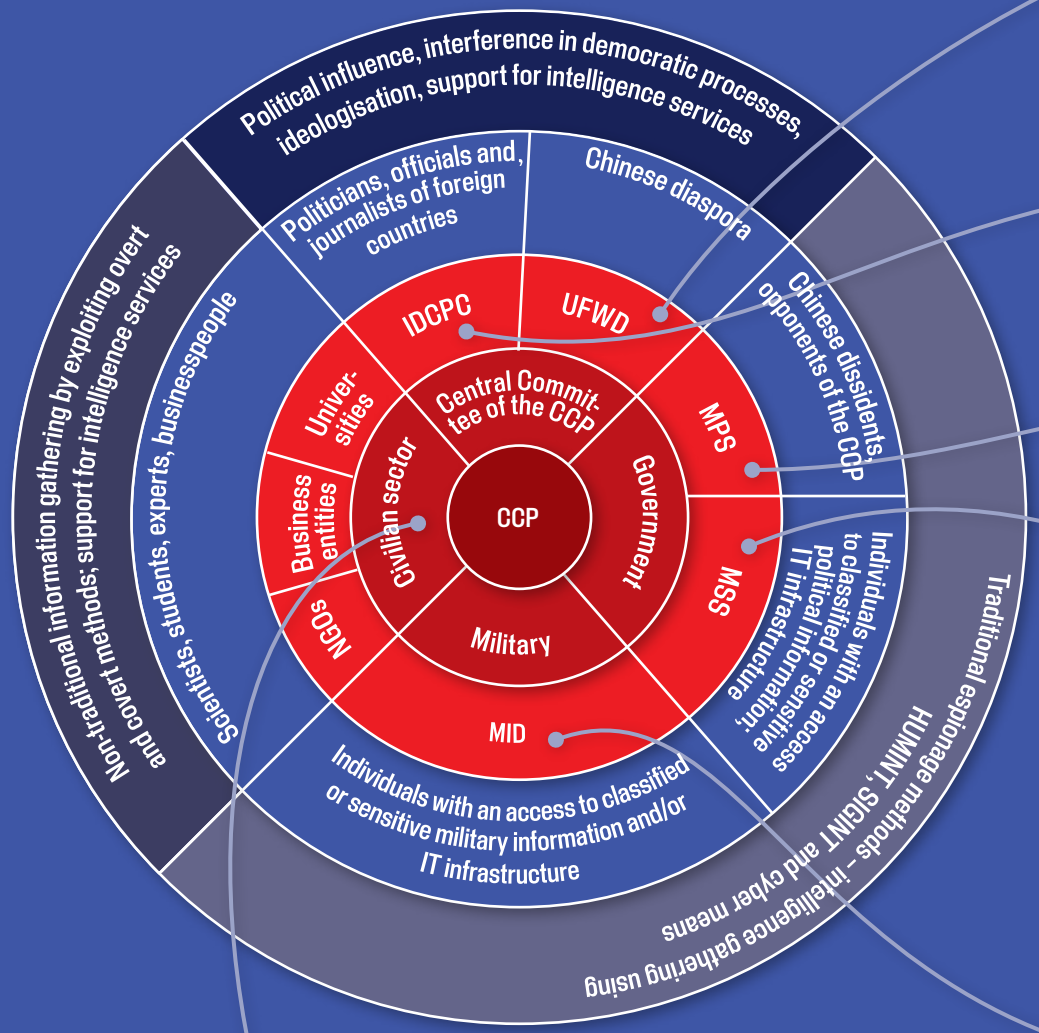
The main task of the IDCPC is to develop relations with foreign countries' politicians, political parties and officials in order to gain international support for China's foreign policy. The IDCPC seeks to influence its contacts to advocate for China in their countries by promoting a positive image of China, helping to ensure the legitimacy of the CCP and China's territorial integrity, downplaying China's human rights abuses, and supporting China on the issues related to the 'five poisons'. Similar to traditional Chinese intelligence services, IDCPC representatives usually present themselves as diplomats and do not declare their affiliation with the IDCPC.

Since IDCPC staff use diplomatic cover, foreign politicians and officials are usually unaware that the Chinese representative has a broader agenda than just developing diplomatic ties. IDCPC staff use their network of contacts to collect information of interest to the CCP: national decision-making on issues affecting China; activities or initiatives of opposition political organisations and individuals; and relations with the Taiwanese, Hong Kong, and Tibetan communities. The IDCPC motivates its contacts by inviting them to events in China and offering to reimburse their travel and leisure expenses during the trip. It is highly likely that the IDCPC assists Chinese intelligence services by

identifying targets for recruitment and acting as an intermediary in establishing contacts between Chinese intelligence services and their potential assets.

The UFWD is the CCP's main tool for developing relations with the Chinese diaspora abroad and mobilising them to support the CCP and marginalise its opponents. The UFWD coordinates a wide network of secondary associations that Chinese living abroad are encouraged to join (e.g. Chinese expatriate or student organisations). These organisations

Chinese regime employs Chinese diaspora to protect its interests
AP / Scanpix



UFWD

In January 2022, the UK's domestic counter-intelligence and security agency, the MI5, issued a public warning that a Chinese citizen, Christine Lee, affiliated with the UFWD, was developing contacts with British politicians. Using various forms of inter-parliamentary cooperation, Lee had been active in British politics for more than 15 years. A law firm set up under Lee's name provided support to selected politicians, amounting to around half a million pounds.

IDCPC

In July 2023, Germany's domestic intelligence service, the BfV, publicly warned German society that IDCPC activity in the country was increasing. According to the BfV, the IDCPC was actively developing contacts with German political parties and members of the parliament with an aim of persuading them to make public announcements and decisions in line with the CCP interests.

MPS

In July 2021, the US Department of Justice accused nine individuals of links to 'Operation Fox Hunt', a programme for monitoring and intimidating Chinese dissidents abroad. One of the defendants, Hu Ji, an employee of Uhan MPS, coordinated a group of people that persecuted Chinese expatriates in the US between 2016 and 2019. Members of the group tracked and blackmailed individuals of Chinese origin threatening to physically harm or execute their relatives if they refused to return to China.

MSS

In November 2021, Xu Yanjun, an MSS employee, was sentenced to 20 years in prison for economic espionage. Using the cover of a Chinese university employee, he established contacts with US aviation industry personnel, coordinated the activities of other MSS agents, sought to identify potential targets working in the US defence sector, and collected economic and technological intelligence. It is assessed that the intelligence information gathered by Xu Yanjun was of great importance to the Chinese aviation industry.

MID

In March 2021, Tarmo Kouts, an Estonian scientist, was sentenced to three years in prison for spying for China. Kouts, who was working in the Estonian defence industry and NATO's underwater research centre, had a security clearance. He was approached by Chinese military intelligence officers using the cover of think tank employees. The scientist managed to only share his views and assessments because the Estonian security service, KAPO, interfered and prevented him from passing on classified information. In return for his information, Kouts was rewarded with free trips to Asian countries, accommodation in luxurious hotels, and dinners in high-end restaurants as well as with financial payments. The total value of the rewards was approximately €20,000.

Civilian sector

In May 2021, Song Guo Zheng, a scientist of Chinese descent, was sentenced to three years in prison in the US. The scientist was the recipient of $4.1 million grant from the US National Institute of Health but had failed to disclose the fact that he had been participating in Chinese *1000 Talents Program* since 2013 and had maintained contacts with Chinese academic institutions, who he shared the findings of his research with. Song was arrested at an airport on his way to China. At the time of the arrest, he had two laptops, three mobile phones, and several USB drives. Song pleaded guilty in the court.

typically have a clear hierarchy and exercise strong ideological control over their members. Organisations coordinated by the UFWD are used to promote narratives favourable to the CCP, to maintain links with the members of the Chinese diaspora and ensure their loyalty and accountability to the Party. Leaders of the Chinese associations maintain close ties with Chinese embassies, where the UFWD officials are usually stationed under diplomatic cover. UFWD staff are responsible for coordinating the activities of Chinese associations, identifying the emergence of anti-CCP sentiment in the associations, and rallying the Chinese diaspora to protest against the decisions or initiatives that the CCP considers contrary to China's interests.

The UFWD also aims to influence political processes and election results abroad. Chinese individuals who have acquired foreign citizenship and the right to vote are encouraged to support candidates of Chinese origin and to protest against politicians or political parties whose agenda is contrary to China's interests. Like representatives of the IDCPC, individuals affiliated with the UFWD collect political intelligence, develop their agency abroad, seek to shape public opinion in favour of China and, highly likely, assist Chinese intelligence services by identifying targets for recruitment.

The legislation regulating the activity of Chinese intelligence services allows them to operate in a 'grey zone' and to use Chinese society and the diaspora for information gathering: students, scientists, professionals working abroad, members of NGOs. This resource is extremely valuable to Chinese intelligence because groups of such individuals have credible cover and can have access to sensitive information or to people who have access to such information.

The CCP seeks to maintain access to Western technology and know-how to enhance its economic competitiveness and accelerate military modernisation. The CCP uses both traditional intelligence capabilities and non-traditional collectors to achieve these goals. For example, by implementing the policy of military-civil fusion, the CCP uses universities affiliated with the Chinese defence sector for espionage and covert acquisition of Western technology and knowledge. Due to the obligation to cooperate with Chinese intelligence, Chinese scientists and students working or interning abroad become potential targets of Chinese intelligence.

China has a keen interest in Western scientific innovations and their application in areas such as artificial intelligence, big data processing, quantum computing, cloud systems, semiconductors, biotechnology, telecommunications, new energy resources, and aviation. China is gathering information on these technologies not only through intelligence methods but also through lawful means: by conducting joint research with foreign scientists, setting up joint research laboratories, establishing joint capital companies, and recruiting scientists to work in China.

Chinese intelligence uses Chinese scientists working abroad for espionage
SIPA / Scanpix

Artificial intelligence technologies as the means of China's pursuit of global technological leadership

China's strategic goal is becoming the global leader in artificial intelligence (AI) by 2030. China is developing ambitious plans according to which AI would accelerate its digital revolution and ensure its global dominance in technological race with the US.

Currently, China is using AI technology to analyse big data, process natural language, develop autonomous and other weapons systems. As a result, China is able to exert tighter control over society, to increase the effectiveness of decision-making, to generate a content that could be used for cyberattacks or to strengthen military capabilities. As AI technology is versatile, China is pursuing global dominance in the AI through a complex of measures:

LEGAL FRAMEWORK

Since 2020, China has tightened the regulation of emerging and disruptive technologies and the companies that develop them. In recent year, the National Data Bureau has been established, and measures for management of generative AI services as well as regulations for deepfakes have been introduced. The new regulation strengthens the regime's efforts to control digital content and data collection and to oversee the application of AI.

THE POLICY OF TECHNOLOGICAL PROGRESS

A rapid development of AI technology in China is mostly determined by the size of the market, government subsidies for state-owned enterprises and AI projects as well as investment in technology hubs and research laboratories abroad. AI research in China is based on military-civil fusion that integrates different entities from both of these sectors – enterprises, universities, and other non-military institutions.

GLOBAL TECHNOLOGY STANDARDS

In 2023, Xi Jinping announced the launch of the Global AI Governance initiative. The aim of the initiative is to ensure equal rights for different countries in the development of AI technology. However, by initiating global regulations and shaping trends of technological development, China aims to create a favourable technological environment in the long term: the introduction of information and data governance based on state control.

THE DOCTRINE OF INTELLIGENTISED WARFARE

According to Chinese defence plans, conventional warfare is gradually shifting to cognitive warfare, defined as the use of public opinion, psychological and legal means to achieve a victory. Although military actions that directly affect the cognitive function and emotions of an adversary is nothing new, AI makes such means more effective and difficult to detect, and therefore more threatening.

INFLUENCE ACTIVITIES AGAINST LITHUANIA

- The effectiveness of cyber-attacks is exacerbated by a lack of attention to cyber-security.

- The quality and frequency of information attacks against Lithuania, Latvia, Estonia, and Poland have increased significantly. These aggressive information operations are aimed at spreading fear among society members and disrupting work of state institutions. Aggressiveness of Russia's information policy is likely to increase further.

- Russia seeks to circumvent sanctions imposed on its propaganda by setting up clones of the restricted websites and disseminating propaganda through social media.

New malicious actors target important Lithuanian decisions in cyberspace

In the war against Ukraine, Russia seeks to influence the West's resolve to support Kyiv through unconventional means. Lithuania's continued support for Ukraine, its NATO membership and its strategically sensitive geographic location make the state a target for Russian cyber operations.

In recent years, the list of groups coordinated by intelligence services of hostile countries, which are monitored in Lithuanian cyberspace, has expanded with new actors, namely a group coordinated by the GRU. This group is characterised by aggressive, destructive attacks. Perpetrators carried out attacks against private sector IT companies providing services to Lithuania's critical infrastructure and state institutions. It is highly likely that the clients of these companies rather than the companies themselves were the intended targets.

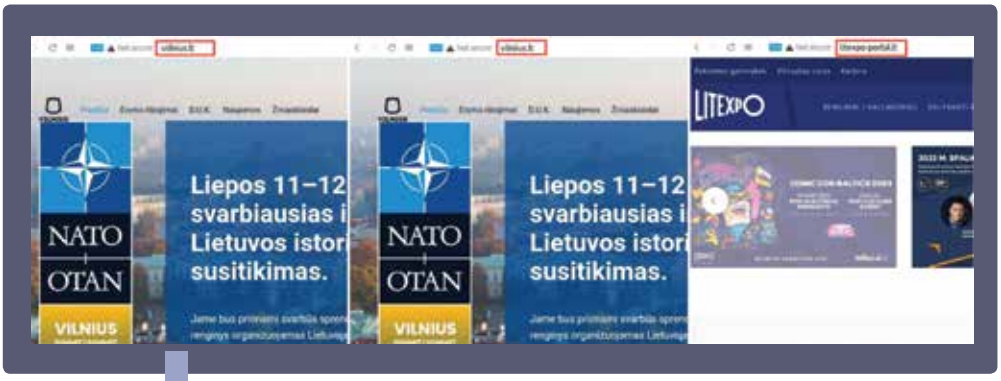
Private sector companies are likely to be more attractive targets, as it is easier for attackers to access the information systems that store their customers' data. Supply chain security is likely to require increasingly greater attention to ensure cyber security.

The Vilnius NATO Summit was also targeted by pro-Russian cyber groups and actors linked to Russian intelligence. Most of the attempts to disrupt the event by cyber means were limited and short-lived. For example, the disruption of systems by DDoS attacks and the dissemination of disinformation through malicious emails were observed. Attempts to create copies of the NATO Summit websites that could be used for malicious activities were identified and thwarted. However, more serious attacks also took place. It is very likely that a cyber group coordinated by the GRU released intercepted non-public information related to the meeting, most likely in order to discredit Lithuania in the international arena. It is possible that some of the intercepted information will be used to plan new disinformation operations.

Russia has been testing new methods of operating in Ukrainian cyberspace for a decade, but the most intense attacks have been carried out in support of Armed Forces operations. For example, since 2022, Russia has been using cyber means to gather information for conventional operations, to disrupt the ability of the Ukrainian Armed Forces to communicate, and launch destructive cyber-attacks against systems controlling electricity supply and telecommunications. Russian cyber capabilities also disseminate fake news by replacing authentic information on Ukrainian media and institutional websites with false data. The aim is to expand the dissemination of disinformation content and increase psychological pressure on Ukrainians.

Chinese cyber groups are also reacting to events related to Lithuania. Their activity in Lithuanian cyberspace has increased especially since 2021, when Lithuania announced the opening of the Taiwanese Representative Office. It has been identified that the previously opportunistic activities of Chinese cyber capabilities, more often directed against the private sector, have been replaced by an active and coordinated effort to gain access to the information systems of Lithuanian institutions for cyber espionage.

It is highly likely that Russian and Chinese cyber capabilities will remain a threat to the security of information networks and systems of Lithuanian institutions and critical infrastructure. Hackers will look for new security vulnerabilities unknown to the cybersecurity sector in order to gain illegal access to targeted organisations. However, it is highly likely that attackers will also use the proven attack methods, the effectiveness of which is enhanced by insufficient attention to cybersecurity.



Examples of fake websites prepared for a foiled malicious cyber operation

Aggressive information attacks seek to intimidate Lithuanian society

Russia employs information warfare to confront the West, viewing it as a continuous activity against its opponents whose policy allegedly oppose Russia's strategic interests. Russia consistently conducts complex information campaigns, including psychological influence and cyber-enabled information operations, to influence the mindset, attitude, and behaviour of the target audience. These campaigns not only involve the spread of false information but also the use of cyber or kinetic elements.

Since 2017, Russia or its associated subjects have been carrying out cyber-enabled information attacks against Lithuania. By 2022, dozens of information attacks involving the dissemination of false information aligned with Russian interests had been carried out. These attacks had no wider impact, as most of them were unsophisticated and used primitive and easily identifiable narratives to discredit Lithuania's national defence or the NATO alliance.

In 2023, the quality and frequency of information attacks began to increase significantly. Lithuania, Latvia, Estonia, and Poland faced unprecedented information operations that included kinetic elements

ATTACKS IN LITHUANIAN INFORMATION SPACE IN 2023

to increase the impact. Compared to the previous attacks, these information operations were more aggressive and aimed at spreading fear and panic among society members, disrupting work of state institutions and inciting dissatisfaction with government decisions as well as the ability to enforce public order. These attacks against Lithuania, Latvia, Estonia, and Poland had a significant impact on society and required a large amount of institutional resources to withstand. An example

of such an information attack involved the dissemination of false information about explosives planted at schools. The attack was timed to coincide with the start of the academic year and the ongoing teachers' strike. Information attacks are usually based on relevant events and exploit contentious issues as well as significant historical events. For example, on the Eve of 9 May, when Russia celebrates victory over Nazi Germany, several statues commemorating the anti-Soviet movement were defaced in Lithuania, Latvia, and Estonia.

Cyber capabilities are often used to conduct information operations. They allow the perpetrators to reach their target efficiently and quickly, to mimic primary information sources, to ensure the efficiency of the campaign, and maintain the anonymity of the campaign organisers. These information attacks do not require significant human or financial resources or specific IT skills.

In 2023, information attacks intensified not only against the Baltic States and Poland but also against other European countries. It is possible that they were carried out by actors affiliated with or coordinated by Russia. Russia's information policy is likely to intensify further. Information attacks in Lithuania will affect a large part of society and hinder functioning of state institutions. It is likely that attacks planned by Russia-linked actors will coincide with the upcoming Lithuanian elections. It is possible that information attacks will be aimed at inciting fear in society, undermining trust in public security institutions, and hindering support for Ukraine.

Russia seeks to circumvent restrictions on its propaganda tools

While the majority of Western countries impose restrictions on Russian propaganda and limit access to sources that disseminate it, Russia seeks to circumvent these sanctions by setting up clones of the restricted propaganda websites that continue to spread propaganda narratives.

In response to restrictions placed on its TV channels and websites, Russia has increased the spread of its propaganda through social media platforms such as *Telegram* and *TikTok*. Russian state-owned or state-controlled propaganda media outlets, their well-known

By spreading propaganda Russia seeks to undermine the will of Western societies to support Ukraine

The main propaganda narratives that Russia continues to use and has been spreading since the start of its invasion of Ukraine downplay the impact of Western sanctions on Russia's economy, incite hatred against Ukraine and its people, and seek to fuel confrontation among Western countries. In addition, Russia also promotes less popular narratives or creates new ones depending on the situation:

'WAR IN THE BALTIC STATES IS IMMINENT'. Russian propaganda tries to convince that the West will use the Baltic States as a bridgehead for the military invasion of Russia but will be unable to defend them after Russia's retaliation. Following the deployment of PMC Wagner mercenaries in Belarus, the narrative that this group was capable of carrying out an independent invasion of Lithuania was spread.

'SUPPORT FOR UKRAINE IS POINTLESS'. The spread of propaganda narratives denying the combat capabilities of the Ukrainian Armed Forces has increased as Ukraine's military actions on the front line have failed to yield any significant territorial gains. The propaganda claims that Ukrainian military and civilian population have lost their motivation to fight and are only being forced to do so by the West-controlled Ukrainian government; and therefore further support for Ukraine's war effort (especially fundraising campaigns by non-governmental organisations) is pointless.

'THE WAR IN UKRAINE IS OF NO IMPORTANCE TO THE WEST'. After the outbreak of Israel–Hamas war, Russian propaganda began to spread the narrative that the armed conflict in the Middle East was much more important for the West than the war in Ukraine. Therefore, Western countries will not only suspend military, financial and humanitarian aid to Ukraine but also will lose all interest in Ukraine.

employees, and individuals from Western countries disseminating propaganda narratives have taken advantage of the lenient approach of these social media networks towards the dissemination of hate speech and war propaganda.

Russia is attempting to intensify its information war against the West by launching new projects to broadcast propaganda from its territory. In July 2023, the Russian state-owned holding RT launched Sputnik radio broadcasts from the Kaliningrad region which reached the Lithuanian regions bordering Russia. The Russian regime considers the implementation of this project a priority.

New Russian history textbooks embody Russia's strategic goals that threaten regional security

History textbooks are an important tool for implementing Russia's history policy. They establish ideological foundations for the strategic goals of domestic and foreign policy. The new history textbooks published in 2023 for 10th and 11th graders present Russia's strategic goals, which will shape the regional security environment in the long term and subsequently affect Lithuania's national security interests.

History textbooks are an efficient tool for shaping historical memory in autocratic and anti-pluralistic Russia. The Russian government views young people as a vulnerable social group due to their lack of support for government decisions. In comparison to the older generation, Russian youth tend to follow independent information sources rather than state-controlled propaganda. According to the regime's perspective, this trend could be mitigated by enhancing ideological education in schools, by using history textbooks as foundation for this indoctrination.

The new Russian history textbooks are much more politically oriented than their previous editions. Their aim is to instil loyalty to the regime's policies and negative attitude towards the West among the youth.

The new history textbooks promote the cult of a strong leader to strengthen the Russian society's obedience to the regime and portray the incumbent autocratic leaders in a positive light. They also justify the Russia's war against Ukraine as a necessary defence against perceived threats. Furthermore, the textbooks present some South-East Ukrainian territories as part of Russia, implying a strategic goal to occupy these territories and cut off Ukraine's access to the Black Sea.

The textbooks present Russia as a civilisation in conflict with the West, suggesting that Russia aims to establish a multipolar world order consisting of anti-Western civilisations, which would secure Russia's exceptional rights in strategically significant regions. In the long term, the Russian government expects that the textbooks will shape society's attitude towards a long-term confrontation with the West and justify numerous resources allocated for this purpose.

Vladimir Medinsky, an aide to the President of Russia and a proponent of a politicised view of history, presents the newly published Russian history textbooks
AFP / Scanpix

CRISIS REGIONS

- The end of the Nagorno-Karabakh conflict reduces Russia's ability to use its levers of influence against countries in the region.
- The Iranian regime's exploitation for the escalation between Israel and Hamas threatens the stability of the Middle East region.
- Due to international pressure to de-escalate tensions, Serbia and Kosovo are continuing their dialogue but are not ready to truly normalise relations and implement agreements.
- In the African Sahel, the rise of military regimes and increasing instability are drastically reducing the influence of Western countries.

After Azerbaijan took control of Nagorno-Karabakh without fighting, Russia lost an important tool for destabilising the region

After the failure to reach a negotiated peace agreement in the long-running conflict over Nagorno-Karabakh between Azerbaijan and Armenia, Baku used favourable circumstances to resolve the conflict by military means. In September 2023, Azerbaijani forces took control of the whole of Nagorno-Karabakh in a 24-hour military operation. The vast majority of Armenians who used to live there have left the region. In the short term, a peace agreement and opening of transport routes through Armenia will remain key issues in the countries' relations.

One of the factors behind Baku's success is the heightened tension between Armenia and Russia. Relations between the two countries deteriorated after the second Nagorno-Karabakh war in 2020, when Moscow reneged on its commitments and allowed Azerbaijan to take control of part of Nagorno-Karabakh. Moscow's posture led to a rise in anti-Russian sentiment in Armenia and allowed the country's leadership to publicly state its intention to change the direction of its foreign policy. In response, Russia increased pressure on Yerevan in order to demonstrate that it was still the main guarantor of security in the region. Despite the apparent confrontation between Russia and Armenia, the latter remains largely dependent on Russia.

In the absence of the Nagorno-Karabakh conflict, Russia's influence in the region will diminish. Since the collapse of the Soviet Union, Russia's main objective in the South Caucasus has been to keep the conflict zones frozen and thus prevent the West from gaining influence. Since the end of the conflict, Russia no longer has a key instrument of power to manipulate the interests of the parties to the conflict. However, Russian military bases in Armenia and the occupied regions of Georgia will allow Moscow to retain some leverage over the countries in the region.

Western Balkans: heightened tensions in Kosovo will require further efforts by the international community

The unresolved issue of Kosovo's statehood and the frozen conflict are causing tensions in the Western Balkans. Pristina's drive to assert its authority over Serb municipalities in northern Kosovo and Serbian protests in 2023 have escalated into violent clashes, including dozens of NATO peacekeepers' (KFOR) injuries. An armed attack by a Serbian paramilitary group against Kosovo police has also increased tensions. KFOR forces have been reinforced in northern Kosovo due to incidents and the risk of escalation.

Pristina accuses Serbia of seeking to destabilise northern Kosovo, while Belgrade widely uses the narrative of persecution of ethnic Serbs in Kosovo. Serbia's close partnership with and energy dependence on Russia, which allows the latter to maintain its influence in the Balkans and use it to increase its geopolitical confrontation with the West, also pose long-term challenges.

In a context of high mutual mistrust, no breakthrough is possible in the near term. Belgrade and Pristina are engaged in an EU-mediated dialogue because they are seeking EU membership and are under international pressure, but are not ready to truly normalise relations and implement agreements. Peace and stability in the Western Balkans will therefore require further international diplomatic, economic, and military measures.

As the conflict between Israel and Hamas continues, Iran's malign activities threaten the region

The unprecedented Hamas terrorist attack in Israel has changed the course of the Middle East conflict. Until 7 October 2023, the Israeli government had believed it could contain the threat of Palestinian terrorism in the Gaza Strip and tolerated the existence of Hamas. After the attack, Israel vowed to eliminate the group and demilitarise the enclave. This shift significantly reduces the possibility of

IDF operating in Gaza Strip
Reuters / Scanpix

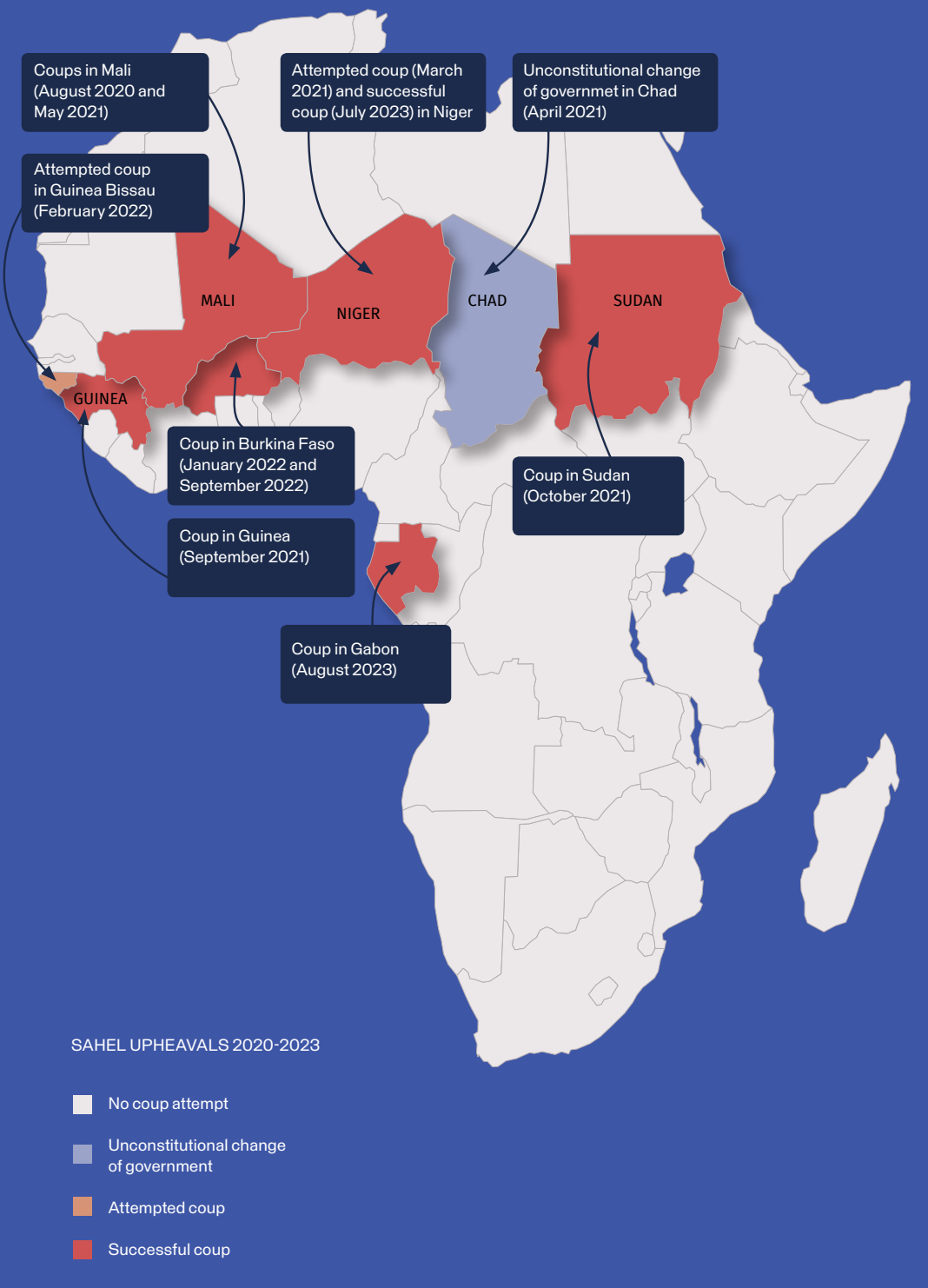
negotiations between Israel and the Palestinians and a diplomatic solution.

The security situation in the wider region has deteriorated as the Iranian regime, Hamas's main foreign backer, continues its campaign of asymmetric warfare. Tehran, keen to maintain plausible deniability, uses various proxies to target Israel and Western interests. Lebanese Hizballah regularly attacks northern Israel. Yemen's Houthi rebels threaten commercial shipping in the Red Sea. Pro-Iranian elements launch rockets and one-way attack drones at US military bases in the region. These attacks are designed to show solidarity with the Palestinians, harass Israel and US troops without provoking a serious response. They increase the risk of further escalation. However, direct involvement of Iran and its proxies in the Gaza conflict remains unlikely at present.

The Israel-Hamas conflict and various related issues continue to have a global impact. Maritime trade in the Red Sea is being disrupted by Houthi attacks. Societies around the world face rising anti-Semitism, including violent incidents, and Islamophobia. The conflict also shifts part of public attention away from the Russian war against Ukraine, creating additional risks for Kyiv.

Africa: coups, insecurity and declining Western influence in the Sahel

In the Sahel, the expansion of military regimes and increasing instability are drastically reducing the influence of Western countries. In Africa, military coups have taken place in Burkina Faso, Mali, Chad, Guinea, and Sudan since 2020, and in Niger and Gabon in 2023. The conditions for military coups are conducive to dysfunctional democracies, weak institutions, frustration with the poor governance of long-standing leaders, prevailing poverty, corruption, and insecurity. International and regional institutional responses (e.g. economic sanctions) make life harder for ordinary people but have no deterrent effect, while the success and impunity of military coups inspire the military in other African countries. There is a tendency for


Coups in Mali (August 2020 and May 2021)
Attempted coup (March 2021) and successful coup (July 2023) in Niger
Unconstitutional change of governmet in Chad (April 2021)
Attempted coup in Guinea Bissau (February 2022)
MALI
NIGER
CHAD
SUDAN
GUINEA
Coup in Burkina Faso (January 2022 and September 2022)
Coup in Sudan (October 2021)
Coup in Guinea (September 2021)
Coup in Gabon (August 2023)
SAHEL UPHEAVALS 2020-2023
No coup attempt
Unconstitutional change of government
Attempted coup
Successful coup

coup plotters to claim to be taking power on a temporary basis in the interests of the state and its people. However, they often later renege on agreements to return to the constitutional order. As military regimes struggle to hold on to power, the prospects for democracy become even more distant.

Growing instability and hostile sentiments reduce the West's ability to influence the security situation in the region. The military juntas in Mali, Burkina Faso, and Niger have taken advantage of the anti-French sentiment, which has grown in public opinion in recent years, and have also forced the withdrawal of French and international forces. In 2023, the West had to come to terms with the loss of Niger as a former security partner and a reduced capacity to conduct counter-terrorism operations in the region. The West's footprint in the region has been reduced by the decision of these African states to expand cooperation with Russia.

The development of terrorist hotbeds and armed conflicts increases overall insecurity and the risks to Europe of increased terrorism and migration. The widespread presence of radical groups in Mali, Niger, and especially Burkina Faso poses a risk of terrorist attacks in neighbouring countries. After the withdrawal of a decade-long UN peacekeeping mission in Mali, the Malian army is being assisted by mercenaries of the Russian PMC Wagner to take control of northern towns. The breakdown of the peace agreement with local Tuareg groups in northern Mali risks a renewed armed conflict. This would increase instability in the region and provide an opportunity for radical Islamist groups linked to Al Qaeda and the Islamic State to gain further ground.

TERRORISM AND MIGRATION

- The threat of Islamist terrorism in Europe is growing. Islamist propaganda, which has intensified in response to the Quran burnings and the renewed conflict between Israel and Hamas, contributes to the increased probability of terrorist attacks.

- Although radicalisation of Muslim community in Lithuania remains low, the presence of Islamist propaganda online does pose a risk of individual radicalisation.

- The Belarusian and Russian regimes exploit the illegal migration to retaliate against the EU and some of its member states and continue to tolerate human smuggling. In the short term, Russia and Belarus highly likely will continue to serve as transit countries for migrants seeking to enter the EU illegally.

Threat of Islamist terrorism in Europe is growing

The period of relative peace in Europe, when Islamist attacks were comparatively rare, is coming to an end as the threat of Islamist terrorism is growing. In 2023, the number of people arrested for planning terrorist attacks has increased. Islamist propaganda, which has intensified in response to the Quran burnings and the renewed conflict between Israel and Hamas, contributes to the increased probability of terrorist attacks. In response to these trends, the Netherlands, France, Sweden, Austria, Slovenia, Belgium, and other EU countries have raised their terrorist threat levels.

The Islamist terrorist organisations Al-Qaeda and the Islamic State, along with their affiliated terrorist groups, are still planning and aspiring to carry out terrorist attacks in Europe. However, they are facing difficulties in rebuilding necessary capabilities for coordinated attacks. Terrorist organisations disseminate propaganda to radicalise Muslims in the West and incite them to carry out terrorist attacks. The most effective propaganda narratives focus on the events that resonate within Muslim communities. For example, propaganda messages that exploit Quran burnings to indoctrinate the audience into believing that Western societies humiliate Islam and persecute Muslims. Propaganda about the conflict between Israel and Hamas aims at mobilising Muslims to act against Israel and its Western allies. Muslims who have failed or have no intension of integrating into Western societies are particularly susceptible to such propaganda narratives, and some may be motivated to carry out terrorist attacks. In 2023, four attacks in Spain, France, and Belgium were carried out by radicalised lone wolves.

The situation in the Middle East has had a significant impact on heightened tensions in European societies, where confrontations between Muslim communities, left-wing Palestine supporters and right-wing anti-immigration activists are on the rise. Pro-Palestinian protests in some European countries have led to anti-Semitic attacks and increased public support for Hamas. Supporters of Palestine in Lithuania protested peacefully and showed no violence or public support for Hamas.

Most European countries have strengthened security around synagogues and other Jewish institutions in response to increased threats
Ap / Scanpix

The terrorist threat in Europe is likely to increase in the near term. The main risk comes from lone radicalised individuals motivated not only by traditional Islamist narratives on the persecution of Muslims but also the deterioration of the situation in the Middle East. Islamist extremists likely will target large crowds, individuals, police officers. The Jewish community and sites related to Jewish culture, history, education, religion, and business are also likely to be targeted because of the Israel and Hamas conflict. Lone extremists do not typically have direct contact with terrorist organisations, nor do they receive financial support or training from them, and are likely to use easily available means, such as knives, cars, or firearms.

Although radicalisation of Muslim community in Lithuania remains low, some foreign nationals from third countries residing in Lithuania have been identified as holding radical views. Although they currently have no intention of using violence, they do not accept democratic values and express anti-Western and anti-Semitic views. There are currently no foreign Muslim organisations, movements, or support groups operating in Lithuania that could spread Islamist ideology in Lithuania. However, the presence of such propaganda online and the continued tension in the Middle East possibly will increase the risk of individual radicalisation and potential terror attacks in Lithuania.

Terrorist and extremist organisations use 3D printing and AI

3D printing and AI, primarily designed for commercial or individual use, also can be exploited by terrorist and extremist organisations. The chatbot ChatGPT, a natural language processing platform, provides opportunities for these organisations to mimic human online conversations, including answering questions, interpreting and processing information, and offering opinions on various topics. 3D printing is a cost-effective and accessible technology that can be employed to manufacture a variety of objects. These technologies are attractive because they are relatively low-cost and easy to use, and do not require specific training. 3D printing and AI enable terrorists and extremists to carry out their activities with greater efficiency, speed, and reduced risk of detection.

3D printed gun parts
Marina Grigorivna / Shutterstock

Logo of ChatGPT Zuma
Press, Inc. / Scanpix

3D printing

USED BY

Mostly right-wing extremists

USED FOR

Manufacturing firearms, explosive weapons and drone parts

AI tools

USED BY

Terrorist and extremist organisations

USED FOR

Creating instructions and itineraries

Increasing the efficiency of information operations by creating personalised propaganda, conspiracy theories and disinformation

Writing programming code for simple cyber attacks

Russian and Belarusian regimes exploit illegal migration facilitated by human smugglers

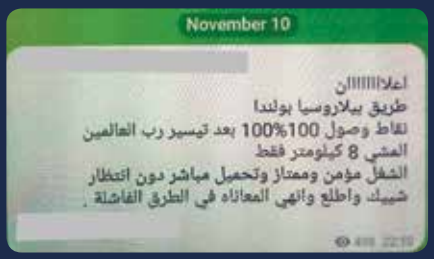
The Belarusian and Russian regimes exploit the illegal migration, which has become a profitable business for human smugglers, for political purposes. Their aim is to retaliate against the EU and some of its member states for their political positions, criticism, sanctions, and other actions that these regimes regard as hostile. In 2023, Russia highly likely used migration against Finland in response to its policy towards Russia, support for Ukraine, and accession to NATO.

Migrants cross the border between Russia and Finland on bicycles
Lehtikuva / Scanpix

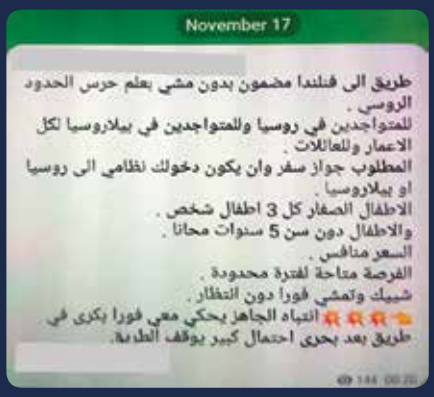
Human smugglers have taken over the organisation of migration via the Eastern Land Route

Human smugglers promote the Eastern Land Route to the EU via Belarus to migrants, as the Belarusian regime tolerates this activity and creates favourable conditions for illegal entry into Latvia, Lithuania, and Poland. Human smugglers are continuously improving their methods, actively promoting the Eastern Land Route on social media platforms, where they offer their services. In chat groups for migrants human smugglers advertise their ability to obtain necessary documents, such as a confirmation of admission to a Russian university or a student visa. Additionally, private *WhatsApp*, *Facebook*, or *Telegram* groups contain advertisements offering jobs for drivers to transport migrants across the border. Typically, citizens of third countries with EU residence permits provide such transportation for migrants.

A post on Telegram channel with a job offer for drivers to transport migrants to the EU



A Telegram post advertises an 8-kilometre route from Belarus to Poland with a '100 percent' success rate guarantee



An advertisement for human smuggling from Russia to Finland. It states that the route is suitable for people of all ages and families.

This tactic is reminiscent of the situation in 2015, when the Russian regime attempted to use migrants to force neighbouring countries into negotiations.

The Belarusian regime highly likely will continue to exert pressure on Latvia, Lithuania, and Poland and exploit illegal migration to achieve its goals in the near term. Illegal migration trends from Belarus to the EU constantly change, with both migrants and human smugglers adapting to the situation along the EU border. In the short term, Russia and Belarus highly likely will continue to serve as transit countries for migrants seeking to enter the EU illegally.

Illegal migration to Europe has been increasing for several years, reaching a record high in 2023. The central Mediterranean route, passing through Libya, Tunisia, and Algeria to Italy, remains the primary route for illegal migration to the EU. The situation highly likely will persist in the near term due to military conflicts, instability, complicated economic, social, and demographic situations in many African and Middle East countries as well as an increased number of natural disasters related to climate change.

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

15.02.2024. Circulation: 1,050 units. Order GL-44

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,
Muitinės str., Domeikava, LT-54359 Kaunas District.

www.kam.lt

ISSN 2669-2732

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.