DEFENCE
INTELLIGENCE
AND SECURITY
SERVICE UNDER
THE MINISTRY OF
NATIONAL DEFENCE

STATE SECURITY
DEPARTMENT OF
THE REPUBLIC OF
LITHUANIA

NATIONAL THREAT ASSESSMENT 2022

DEFENCE
INTELLIGENCE
AND SECURITY
SERVICE UNDER
THE MINISTRY OF
NATIONAL DEFENCE

STATE SECURITY
DEPARTMENT OF
THE REPUBLIC OF
LITHUANIA

NATIONAL THREAT ASSESSMENT 2022

VILNIUS, 2022

CONTENTS

INTRODUCTION	3
FOREWORD	5
SUMMARY	8
RUSSIA	12
BELARUS	25
CHINA	30
CONFLICT REGIONS	36
THE ACTIVITY OF HOSTILE INTELLIGENCE AND SECURITY SERVICES	39
CYBER SECURITY	46
INFORMATION SECURITY	52
TERRORISM AND MIGRATION	55
ECONOMIC AND ENERGY SECURITY	61

INTRODUCTION

The National Threat Assessment by the State Security Department of the Republic of Lithuania (VSD) and the Defence Intelligence and Security Service under the Ministry of National Defence of the Republic of Lithuania (AOTD) is presented to the public 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 4 February 2022.

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: 0–6 months	Near term: 6 months – 2 years	Mid term: 3–5 years	Long term: 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,

It gives a great pleasure to present the seventh edition of the National Threat Assessment prepared by the State Security Department of the Republic of Lithuania and Defence Intelligence and Security Service under the Ministry of National Defence of the Republic of Lithuania.

By performing the tasks set by the national State Defence Council, every day we analyse and assess both external and internal threats to our state and society. The constantly changing environment poses challenges from various types of hostile actors to us – be it foreign countries, their armed forces, intelligence and security services, various economic actors, state-sponsored media propaganda or radicalized individuals, prepared for terrorist attacks.

It has been a long time since Lithuania and our transatlantic Allies experienced such a strong pressure from authoritarian states. Alyaksandr Lukashenka's orchestrated migration crisis has become a significant challenge to our state. The self-proclaimed leader of Belarus demonstrates his willingness to further exacerbate the conflict with his Western neighbours. An aggressive Chinese policy will increase economic, cyber and information threats to Lithuania. Meanwhile, Russia is and will remain the greatest and potentially existential threat to Lithuania and other countries of the region. By threatening to invade Ukraine and spark a conflict in Europe, Russia seeks to force the West to acknowledge its right to determine political choices of other independent states to decide on the ways how to ensure national and regional security. Moscow is also taking advantage of instability generated by Lukashenka and together with Beijing further challenging the West.

Our goal is to inform the readers, no matter whether they live in Lithuania or any other country, that hostile spy agencies might attempt to use their knowledge, connections, manipulate their personal interests or weaknesses – all in order to persuade them to betray their own country. In addition, hostile intelligence seeks to hack our devices and to mislead and disintegrate our society by spreading lies. Therefore, we expect that the awareness of hostile intentions and capabilities will help to critically assess the reality and will enable us to become more resilient on society and individual levels.

It comes as no surprise that a majority of daily intelligence work is classified and cannot be disclosed. Consequently, some of our assessments do not reveal the most sensitive details and thus may sound sketchy. Nevertheless, this review presents the essence of threats and challenges that Lithuania and other allied countries are facing and represents closely coordinated work of Lithuanian intelligence community.

15min.lt / Scanpix

SUMMARY

■ **Russia's military potential combined with aggressive policies is the primary external security threat to Lithuania.** The Kremlin continues to oppress any signs of internal opposition in an attempt to ensure domestic political stability – prerequisite for Vladimir Putin's regime survival. Moscow attempts to persuade the country's population that the West is to blame for the economic and social problems and society's discontent with the regime; however, it is clearly an outcome of ineffective political system and poor management of national resources and priorities. Therefore, the regime employs increasingly aggressive tactics in fighting against the perceived internal and external opponents, escalates military threats to neighbouring states and the West thus seeking to allegedly prevent threats to Russia.

■ **Military power is the primary tool for Russia to exercise international influence.** The Russian Armed Forces (AF) and especially rapid decision making enable the Kremlin to intimidate their neighbours with the prospect of military conflict and shape the international security agenda. It also enables Moscow to strengthen negotiating position on important international issues, to check the Western reaction, test the unity, and eventually to respond to developments unacceptable to Russia. The goal of Russia is to convince the international community that it is ready for military confrontation, unless its demands are taken into consideration. The aggressiveness of the Kremlin's regime and consistently strengthening Russia's military potential will further pose the greatest threat to the national security of Lithuania and other countries in our region.

■ **A weakening Lukashenka's regime is increasingly becoming a source of security threats.** Minsk's aggressive policy towards its western neighbours conforms to the Kremlin's interests. Lukashenka's orchestrated migration flow towards Lithuania, Latvia and Poland contributed to Russia's goal to challenge the security of NATO and the EU members. Consequently, after Minsk entered into confrontation with the western neighbours, the country became even more dependent on Moscow. As a response to internal opposition, the authoritarian regime in Minsk is increasingly gaining features of totalitarianism. Russia intensifies military manoeuvres in Belarus and the scope of their military cooperation is growing.

■ **Authoritarian Chinese foreign policy, economic and information activity are becoming increasingly aggressive.** China applies complex counter-measures against the states that establish closer relations with Taipei, express their concern over human rights situation in China, and restrict Chinese investment into strategically important sectors. China exerts pressure by freezing diplomatic relations, degrading the level of diplomatic representation or by creating multiple obstacles for trade and investment. Beijing complements its actions with influence and information campaigns. China used many of these coercive means on Lithuania as a result of the decision to withdraw from 17+1 cooperation format and open the Taiwanese Representative Office in Lithuania.

■ **Hostile intelligence activity against Lithuania remains intensive.** Russian and Belarusian intelligence services make every attempt to recruit Lithuanian citizens coming to their countries. They also actively act against the opposition activists and organizations that relocated abroad due to persecutions at home. Moreover, Russian and Chinese intelligence services pursue active espionage in cyber space. By using cyber security vulnerabilities, the hostile services take over information and exploit it for political interests or for information operations.

■ **Russian and Belarusian propaganda campaigners intensified their activities against Lithuania.** Attempts by various propaganda outlets to obtain material for their production have increased. For this purpose, pro-Kremlin political radicals living in Lithuania are usually engaged. An intensive Russian and Belarusian propaganda campaign against Lithuania and other states also played an integral part in migration crisis orchestrated by the authorities in Minsk. Furthermore, foreign propagandists tried to take benefit of large scale protest campaigns held in Lithuania in 2021 and intentionally highlighted the most radical elements of the protest. Attempts to spread pro-Kremlin propaganda in Lithuania were also made by Russian intelligence services.

■ **While a terrorist threat from radical Islamism in Lithuania is low, yet the country is at risk of a terrorist attack, perpetrated by right wing ideology followers.** There are several dozen right wing extremism supporters living in Lithuania, whose activity poses risks to the state security. It is also known that a number of individuals with suspected links to terrorist or extremist organizations have tried to enter Lithuania through illegal migration route from Belarus. In many other EU states, a terrorism threat remains high. A direct terrorism threat in Europe is posed not only by terrorist organizations but also by radical individuals inspired by extremist ideology.

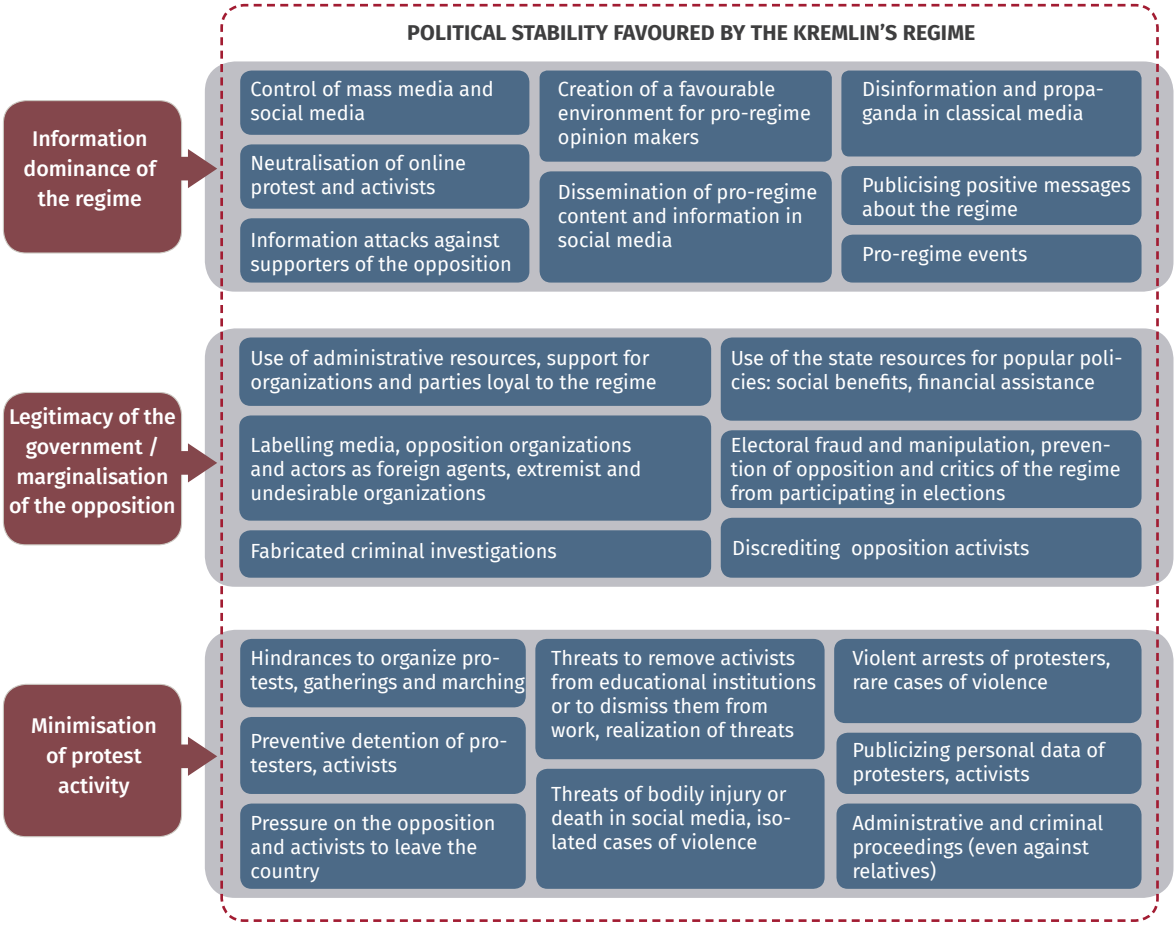
RUSSIA

BY STRENGTHENING REPRESSION, THE KREMLIN SEEKS TO CONSOLIDATE THE REGIME'S POWER FOR DECADES

The Kremlin neutralised the non-systemic opposition and secured the political stability sought-after by the ruling regime. The Kremlin successfully exploited the unrest caused by Alexei Navalny's poisoning attempt and the arrest that followed upon his return to Russia to undermine the opposition activities. Protest supporters were subjected to repression and intimidation indiscriminately, administrative and criminal proceedings were initiated against demonstrators (sometimes for completely unrelated and bogus criminal charges), and a number of activists were put under pressure to leave the country.

Pressure is applied not only on the non-systemic opposition but also on the most popular moderate opposition and even on members of the pro-regime Communist Party (KPRF), who criticize the Kremlin. It has become obvious that the Kremlin no longer tolerates competition, even with the systemic opposition, and seeks to ensure that politicians on all levels of government are fully loyal and subordinate to the regime. The forms of repression are not new; however, they are no longer used against the selected targets, but *en masse*. Neither the opposition's participation in the elections nor any other significant opposition activity are longer possible in Russia.

The ruling regime exerts pressure on independent media at the scale unprecedented even for Russia: the most prominent investigative journalism outlets, TV channel *Dozhd*, and dozens of individual journalists were declared 'undesirable organisations' or 'foreign agents'. The Kremlin perceives any activity supported by the West as a threat; such support provokes the regime's pressure and repression even on non-governmental organisations, which are not related to politics.



The Kremlin's measures to create a conducive political environment and neutralize the opposition

The Kremlin desires to maintain political stability rather than democratic legitimacy. In September 2021 elections, the ruling party 'United Russia' and candidates supported by the government won by a landslide and maintained the constitutional majority in the State's Duma, although this result was reached only by repression, manipulation of the electoral process and falsification of the results. Independent observers and opposition activists criticised the electoral procedures and reported numerous irregularities. However, official institutions rejected criticism and accused the opponents in Russia and foreign actors of attempts to discredit the voting by disinformation and cyber-attacks.

The Kremlin is paying more attention and allocating more resources to fight against the perceived internal and external enemies and to expand the state control in all areas, rather than to increase Russia's openness and attraction, social security and citizens' well-being. The National Security Strategy adopted in 2021 also reflects this trend; it differs substantially from the 2015 edition in its anti-Western rhetoric. In the strategy Russia is presented as a besieged fortress, which the West tries to isolate, it exerts political, economic, information and cultural pressure, as well as seeks to provoke a long-term instability in Russia. The response to these threats is to maintain sovereignty and "traditional values of the Russian nation", to protect itself from external interference in internal affairs and to increase the state capabilities in all areas. In the field of military security, this is expressed in the concept of "active defence", i.e. an active creation of threats to opponents in order to prevent threats to Russia.

By arguing the need to strengthen the state's cyber security, the Kremlin increases the power to control any digital content in the national territory. Russia has developed an influential bureaucratic apparatus responsible for information security issues. Most of the top policy makers in the domain of information security have experience in law enforcement or intelligence services and are currently employed in government agencies or private companies, thus facilitating their close cooperation and interaction.

Vladimir Putin (69 y/o), Secretary of the Security Council Nikolai Patrushev (70 y/o), Director of the Federal Security Service (FSB) Alexander Bortnikov (70 y/o), Director of the Foreign Intelligence Service (SVR) Sergey Naryshkin (67 y/o), Minister of Defence Sergey Shoygu (66 y/o), Minister of Foreign Affairs Sergey Lavrov (71 y/o). In order to keep the aging elite in power, Russia has introduced amendments to the law that currently allow civil servants and officials to hold their positions until they are 70 years old.

TASS / AP / Scanpix

The Kremlin's regime is becoming increasingly authoritarian and heavily relying on the cult of personality. Putin's main supporters in government structures and state corporations (Gazprom, Rosneft, Rostech, Rosatom) remain aging elite composed of relatives or personal friends and their trustees. The nomenclature of the regime assumes that even after the withdrawal of Putin, his model of governance will persist. This shows that the Kremlin does not intend to change its policies characterised by stagnation, internal repression, isolationism and aggression towards other countries, especially the neighbouring ones. These trends increase the long-term threat to Russia's Western neighbours.

RUSSIA THREATENS REGIONAL STABILITY MILITARILY. UKRAINIAN CASE

Along with a stable composition of the Russian political regime, the Kremlin's perception of strategic environment and Moscow's foreign policy goals remain unchanged. One of the Russian priorities is to align the foreign policy of CIS area countries with Moscow's interests. Without any real deterring factors, Russia has continued this effort since the fall of the Soviet Union.

However, the conflict with Ukraine is an important example of such Russian policy not always bearing fruit. On the contrary, the Kremlin's attempt to force Ukraine to succumb to Russian terms has had a negative effect since 2014. Even when Moscow's aggression continues to push Kyiv towards the West, Russia chooses to escalate the conflict further instead of conducting earnest negotiations and abandoning ambitions to undermine Ukraine.

In October 2021, the Russian Armed Forces once again started to deploy military units near Ukraine. They started to deploy troops and military equipment from all Military Districts to Yelnia in Smolensk region, occupied Crimea and other areas near the Ukrainian border. The increased military presence was accompanied by the Kremlin's allegations towards Ukraine and NATO, as well as by demands to grant "comprehensive security guarantees" for Russia. Kyiv was accused of preparing to launch an assault on Donetsk and Luhansk, while NATO received criticism for allegedly instigating Ukrainian aggression, arming Kyiv and conducting military exercises in the Black Sea. These allegations in

effect repeated and even exceeded the Russian rhetoric of spring 2021, when Moscow unexpectedly amassed a large number of troops near the Ukrainian borders and used propaganda to create a perception of imminent invasion into Ukraine.

Concentration of the Russian Armed Forces along Ukraine's border

These Russian actions illustrate the Kremlin's modus operandi – to threaten to invade a sovereign country in order to put it and the international community under pressure to accepting solutions that appease Putin's regime. Military force and readiness to use it are the foundation of Russian international influence, as shown in Ukraine, Georgia, Syria or Nagorno Karabakh. Russian political and military leaders are convinced that a show of force is a useful negotiation tactic to force the opponent to accept Moscow's political demands. As Putin put in November 2021, NATO countries started to pay attention to the Kremlin's 'red lines' only when Russian military units moved towards the Ukrainian border.

Moscow objects to Ukraine's deepening ties with the Euro-Atlantic community, joint military exercises with NATO and Western supplies of lethal armaments to Ukrainian forces. Kyiv's membership in NATO and especially Allied military infrastructure deployment in Ukraine have been numerous times highlighted as Russian 'red lines' that will provoke a reaction from Russia. According to the Kremlin, the only acceptable future for Kyiv is to grant the Russian-controlled Donetsk and Luhansk regions a special status inside Ukraine and relinquish power to define Kyiv's foreign and security policy priorities to Moscow. Aggressive Russian military manoeuvres and rhetoric are aimed to prove to any country, close to Russia politically or economically, that independent policy is tolerated as long as it does not clash with the Kremlin's interests.

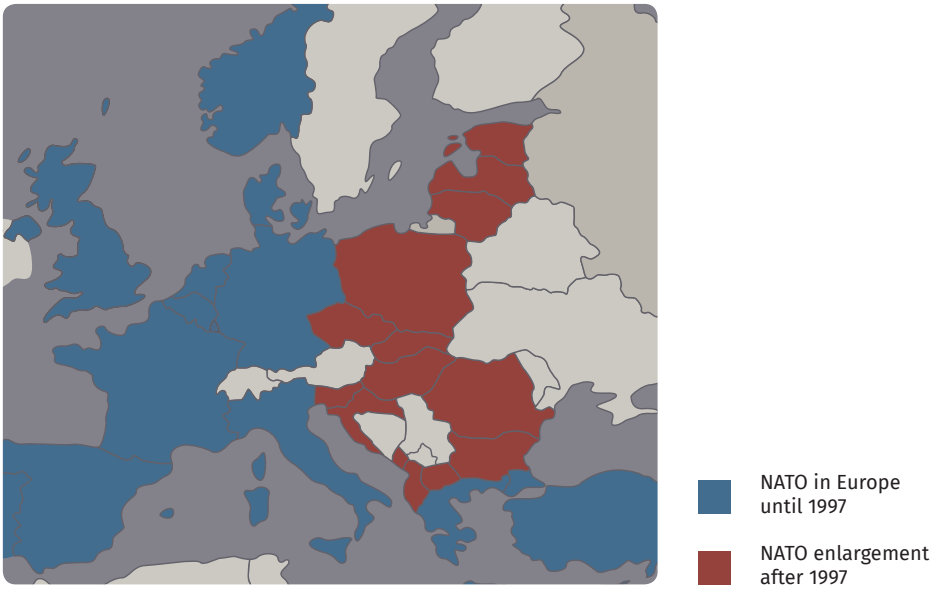
Russian military potential, its ability to deploy forces quickly and centralized decision-making will further enable the Kremlin to use military pressure as a tool to secure Russian national interests. Russia will continue to employ military force to support its negotiating position in various security formats, to gauge possible reactions of the newly elected Western leaders, to demonstrate its frustration with NATO exercises or deployments or to respond to Western sanctions. Thus Moscow will seek to prove to the international community that any attempt to contain Russia will prompt a strict response and the only way towards a sustainable security situation is to submit to Russia's demands.

Threats of quick use of military force are supported by Russia's readiness to rapidly generate forces. It is done by establishing battalion tactical groups (BTGs) of 700-800 soldiers that are ready to execute combat orders with a 24-48-hours' notice. The number of such groups in the Russian Armed Forces is constantly growing – in contrast to 96 BTGs available in 2016, last year Russia reached an ability to form 168 BTGs. These groups, exclusively manned with contract soldiers, are indispensable not only in combat missions, they are also used to demonstrate credible deterring military force in selected regions. Also, the trend of growing military capability was demonstrated by defence minister Sergey Shoygu's announcements last summer that 20 new units were to be formed in Western Military District by late 2021.

It is highly likely that such Russian conduct will continue to inflame tensions in its neighbourhood, including the Baltic Sea region. This will negatively affect the Lithuanian and regional security environment and increase the risk of unintended incidents.

Nevertheless, it is likely that Russia only commences military operations having made sure that possible benefits will outweigh the costs. Military capabilities of potential opponents and NATO security guarantees are the most important factors limiting the Russian military ambitions. Therefore, growing Baltic national and Allied defence capabilities reduce the likelihood of Russia's decision to use military force against the Baltic States.

On 17 December 2021, Russia made public its demands to NATO and the USA thereby seeking to establish its zone of influence, where Russia could limit NATO military activities, gain veto rights in terms of further NATO enlargement and strengthening of NATO defensive capabilities in Lithuania and neighbouring NATO countries.



Russia's main demands to NATO and the USA:

- Not to grant Ukraine and Georgia membership in the Alliance.
- To withdraw NATO military units from the states that have joined the Alliance since 1997.
- Not to conduct larger that brigade-level exercises in vicinity of Russia’s borders.
- Not to conduct any kind of military activities in the territory of Ukraine, Eastern Europe, South Caucasus and Central Asia.
- Not to deploy short and intermediate-range missiles in the territories allowing them to reach targets in the Russian territory.

ROUTINE COURSE OF ZAPAD 2021 DID NOT STOP RUSSIA FROM SENDING A POLITICAL MESSAGE TO NATO

Last year, training ranges in Russia's Western military district and Belarus were traditionally busy with strategic military exercise ZAPAD 2021. The active phase officially lasted from 10 to 16 September but various training elements had been observed since mid-summer.

The declared aim of the exercise was to check the interoperability of the Russian and Belarusian Armed Forces, however, the political context that accompanied the military power demonstration was no less important or even more important to Moscow.

First, Russia highlighted the international character of ZAPAD 2021 and the fact that the number of the invited foreign partners had been the highest of all Russian strategic exercises so far. Although not all the invited nations sent their participants, Moscow aimed to show that Western sanctions did not leave the country in complete isolation and unable to form a coalition of like-minded allies.

Offensive elements in ZAPAD 2021: paradrop of combat vehicles in Kaliningrad Region
Reuters / Scanpix

Moreover, Russia used the opportunity to send several contradictory messages to the West. In their official rhetoric, Russian leaders were moderate and relied on the time-tested message that the exercise was solely defensive, despite some offensive elements playing an important role along manoeuvre defence actions.

Nevertheless, in contradiction to statements about the routine nature of the exercise, Russia declared ZAPAD 2021 a response to Western actions, although strategic exercises take place every year and their scope does not correspond to any supposedly hostile foreign actions.

In addition, Russia demonstrated that its declarations of transparency remain a formality. Although ZAPAD 2021 was conducted as planned, the number of participating troops was once again seriously underreported. According to Moscow's international obligations under the Vienna Document, all activities above the 13,000-troop threshold are subject to observations by other OSCE members. Russia officially declared a lower personnel number under the Vienna Document but at the same time publicly issued an inflated count of up to 200,000 troops. These manipulations showed Russia's willingness to openly circumvent its international obligations, demonstrate the Vienna's Document inability to force Russia to declare the actual size of exercise and intimidate the West.

While the West had their eyes on the large-scale exercise near the eastern NATO flank, Russia voiced their concern over the purported violations of the 1997 NATO-Russia Founding Act. According to Moscow, NATO allegedly should not deploy permanent substantial combat forces on the territories of the new NATO member states. In fact, the document does not carry that obligation except for an agreement not to deploy nuclear capabilities in the former Warsaw Pact countries, while commitment to carry out missions by interoperability, integration, and capability for reinforcement rather than additional forces was only made in the prevailing security environment that Russia itself corroded with its aggressive foreign military endeavours. Russia violates its own Foundation Act obligations to show restraint in deployment of conventional and nuclear capabilities, to comply with arms control agreements and, most importantly, respect sovereignty and territorial integrity of all states. Military operations in Ukraine and Georgia, violations of the INF treaty and the Vienna Document, conventional forces deployment in the Western strategic direction – all Moscow's actions show that it is not willing to comply with agreements that contradict its strategic interests.

As ZAPAD 2021 was approaching its end, Russian foreign minister Sergey Lavrov used the event as an opportunity to present a possible solution to improve the Vienna Document procedures if NATO agreed to withdraw forces from the territories of its new members, including Lithuania, thus returning to the status quo held at the time when NATO-Russia Founding Act was signed. This position in nature contradicts the principle of indivisible security that Russia also agreed to – a notion that countries cannot strengthen their security at the expense of other states. ZAPAD 2021, especially the political rhetoric that accompanied it, shows that Russia ignores its international agreements and will continue to do so as long as NATO allegedly ignores Moscow's considerations.

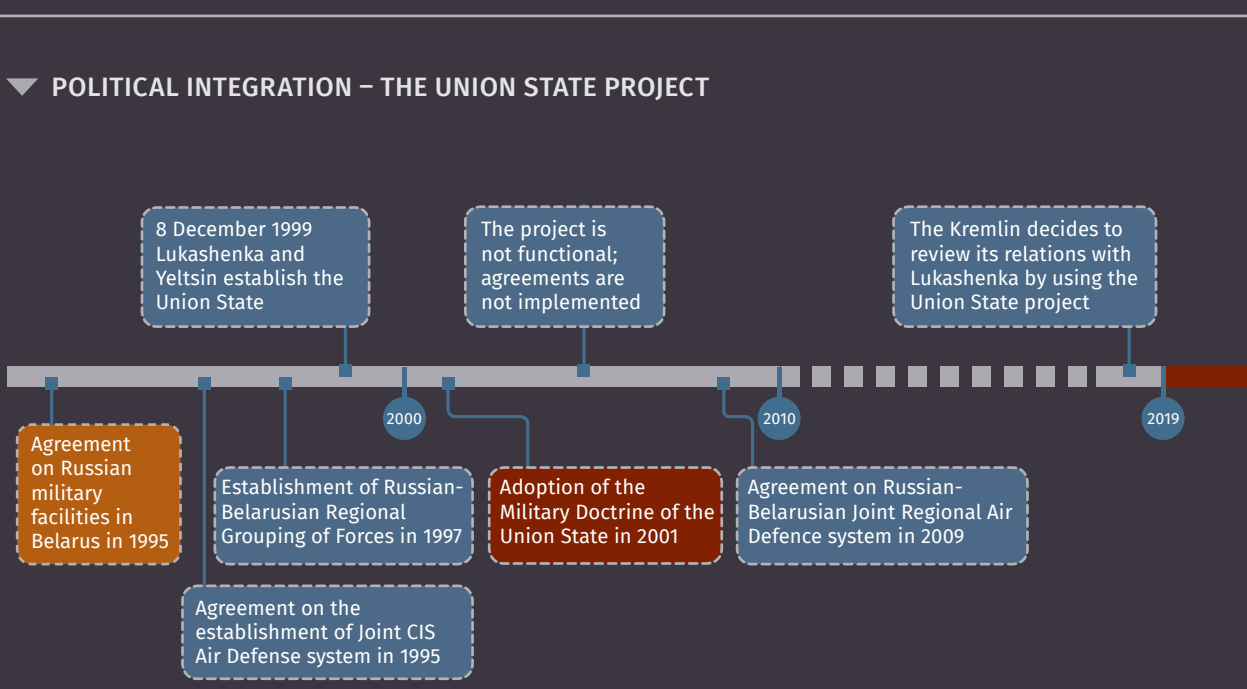
During ZAPAD 2021 Russia attempted to demonstrate military power to the West
AFP / Scanpix

THE KREMLIN BENEFITS FROM LUKASHENKA'S AGGRESSIVENESS TOWARDS THE WEST AS IT MAKES HIM INCREASINGLY DEPENDENT ON RUSSIA

The Kremlin reinvigorated the Union State project at the end of 2018, when criticism against the Belarusian dictator Lukashenka became stronger in Moscow. The Russian financial elite was particularly dissatisfied with various discounts to Belarus, e.g. low natural gas price and various tax concessions. The Kremlin was irritated by Lukashenka's independent foreign policy – Lukashenka did not recognise Crimea as a part of Russia and tried to approach the West in order to counterbalance the Russian influence.

The situation in Belarus has fundamentally changed since. Due to increasing repressions in Belarus and the regime's aggressive foreign policy towards the EU's neighbours, Lukashenka is no longer able to balance between the East and the West. This corresponds with Russian interests. In addition, while negotiating the energy supply terms and programmes of the Union State, Russia reduced financial support to Belarus and closed loopholes that allowed Belarus to pay Russia fewer taxes on the European goods it was re-exporting.

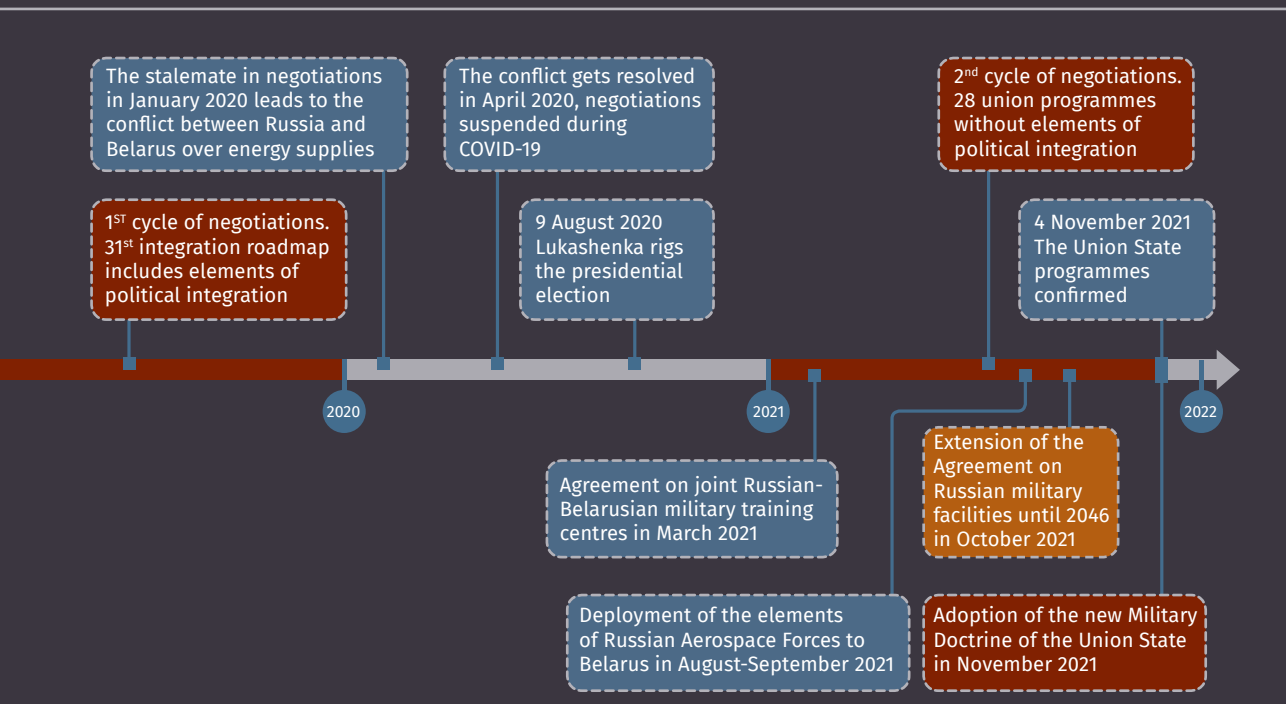
It is highly likely that the Kremlin considers the current situation in Minsk to be stable and will avoid intervening in the internal affairs of Belarus. Political integration of the countries is not envisaged in the near term, nor were such agreements reached during the negotiations over the Union State. However, it is likely that the Kremlin has a long-term goal to increase its influence over Belarus. Russia will try to achieve it by using both the Union State project and other instruments, if necessary.



Belarus and Russia continue to intensify military cooperation. In 2021, Russia deployed the elements of the Aerospace Forces on the Belarusian territory, the two countries revised the military doctrine of the Union State and extended the agreement on the Russian Military facilities (the 43rd Communication Center with Submarines in Vileika and Early Warning Antimissile Station near Hantsavichy) in Belarus for 25 years. Belarus received modern armoured combat vehicles from Russia.

The question regarding the permanent deployment of the Russian Armed Forces (military base) in Belarus has been of concern since 2013, but Lukashenka has always succeeded in rejecting it. This position has changed to some extent due to decreasing Lukashenka's political independence and probably increasing pressure from Russia. In March 2021, the Ministries of Defence of Belarus and Russia agreed to set up three joint combat training centres, with one of them to be established in Belarus for training crews of multirole aircraft Su-30SM (FLANKER H) and air defence personnel able to use modern air defence systems. In January and February 2022, on the pretext of a military exercise, Russia deployed an unprecedented size force package to Belarus. The grouping included ground forces equipped with tanks and artillery, Airborne and Naval Infantry troops, aviation subunits with fighter jets, attack and transport helicopters. Modern air defense systems SA-21 were also deployed. The bulk of Russia's forces arrived from the Eastern military district.

Having deployed military units to Belarus, Russia has reinforced its option to be able to launch an attack into Ukraine from the Belarusian territory. The case illustrates that Russia can exploit the Belarusian territory to implement its aggressive policy towards other countries.



Amid Belarusian regime's escalation of the illegal migration crisis at the EU borders, Russia has shown support for Minsk and demonstrated its dependence upon Moscow to the West. In November 2021, Russia conducted strategic aviation bomber flights in Belarusian airspace and held Airborne Troops exercise, during which 250 Russian VDV troops were paradropped.

BELARUS

LUKASHENKA MAINTAINS POWER THROUGH REPRESSION AND INTIMIDATION

In 2021, Lukashenka maintained power in Belarus and stabilised the regime. The opposition protests have not resumed and it is likely that the regime does not feel any direct internal threats to its survival. In order to preserve the remains of public support and strengthen his chances to retain power for as long as possible, Lukashenka imitates changes in the regime. He pardoned dozens of the arrested protesters, organised a supposed 'Constitutional reform' and announced a new public holiday, the 'National Unity Day'. However, the regime is unlikely to enter into dialogue with the opposition in the near term.

Aiming to control society more effectively, the Belarusian regime amends laws, increases penalties for breaking them and expands the role of the *siloviki* block in the country. Hundreds of Telegram channels, having become a source of news for Belarusians, were declared 'extremist material'. Subscribing or sharing their content poses a risk of being prosecuted by the criminal law. People are persecuted for publicly displaying the national white-red-white flag and the national symbol of *Pahonia*. Members of the opposition are placed on the official terrorist list published by the KGB, and the trusted *siloviki* are being appointed to important positions. To avoid a new wave of protests, the local elections of January 2022 were postponed to 2023, when local and parliamentary elections will be held together. This shows that the regime is not prepared to take risks and is seeking to delay any political system stability tests.

By directing repression at all Belarusian residents, the regime creates a sense of total control and inevitable punishment. The regime persecutes teenagers,

pensioners, teachers, students, factory workers, officials and others who have expressed their criticism publicly or even privately. A 15-day arrest can be given for a white-red-white coloured sticker on the apartment door or a negative comment about law enforcement officers on social media. On the pretext of the pandemic, the right of Belarusian citizens to leave the country is restricted.

In order to clear the information space of damaging messages, the regime pays special attention to opposing Belarusian or even Russian journalists, portals and bloggers. The largest news portal *tut.by* has been blocked while journalists from the independent TV channel *Belsat* operating from Warsaw are being persecuted. The Belarusian regime forced to close the office of the Russian news outlet *Komsomolskaya pravda v Belarusi* after it published an inconvenient article about killing of a KGB officer during the shooting.

Lukashenka's authoritarian regime acquires more and more features of a totalitarian rule. He is no longer satisfied with mere political control of the country, he rather seeks total obedience of all Belarusians in both public and private domains. The Belarusian regime restricts freedom of movement of its citizens, blocks news outlets and closes various non-governmental organisations. Finally, the majority of the country's economy is controlled and managed by the regime or by persons associated with it. Such a regime being based on repression only and deprived of the slightest respect for human life and dignity is a major source of instability in the region.

To simulate public support, a clothing shop with popular phrases by Lukashenka opened in Minsk

Sergei Shelega / BelTA / TASS / Scanpix

LUKASHENKA'S RESPONSE TO SUPPOSED FOREIGN ENEMIES – ASYMMETRIC TOOLS OF INFLUENCE

Lukashenka's long-term goals are legitimisation of his regime and normalised relations with the West. In the near term, Minsk's key objective is to stop the adoption of the new sanctions against the regime, and, preferably, to lift the already imposed ones. In order to achieve his goals, Lukashenka uses various asymmetric tools of influence against Lithuania and other Western neighbours.

Threatening rhetoric

Aiming to intimidate Lithuanian politicians and society, Lukashenka both publicly and via informal channels has threatened well-being of Lithuanian citizens and the security of Lithuanian goods transited via Belarus. There have also been threats of an increased flow of illegal migration as well as tobacco and drug smuggling to Lithuania.

Diplomatic pressure

In response to Lithuania's decision to provide refuge to Belarusian opposition leader Sviatlana Tsikhanouskaya, Belarus expelled almost all the Lithuanian diplomats from Minsk.

Propaganda and disinformation

By disseminating propaganda, the Belarusian regime seeks to justify its actions, discredit and promote distrust in the Lithuanian government and Belarusian opposition. The regime exploits the migration crisis to discredit neighbouring EU countries for alleged human rights violations.

Legal instruments

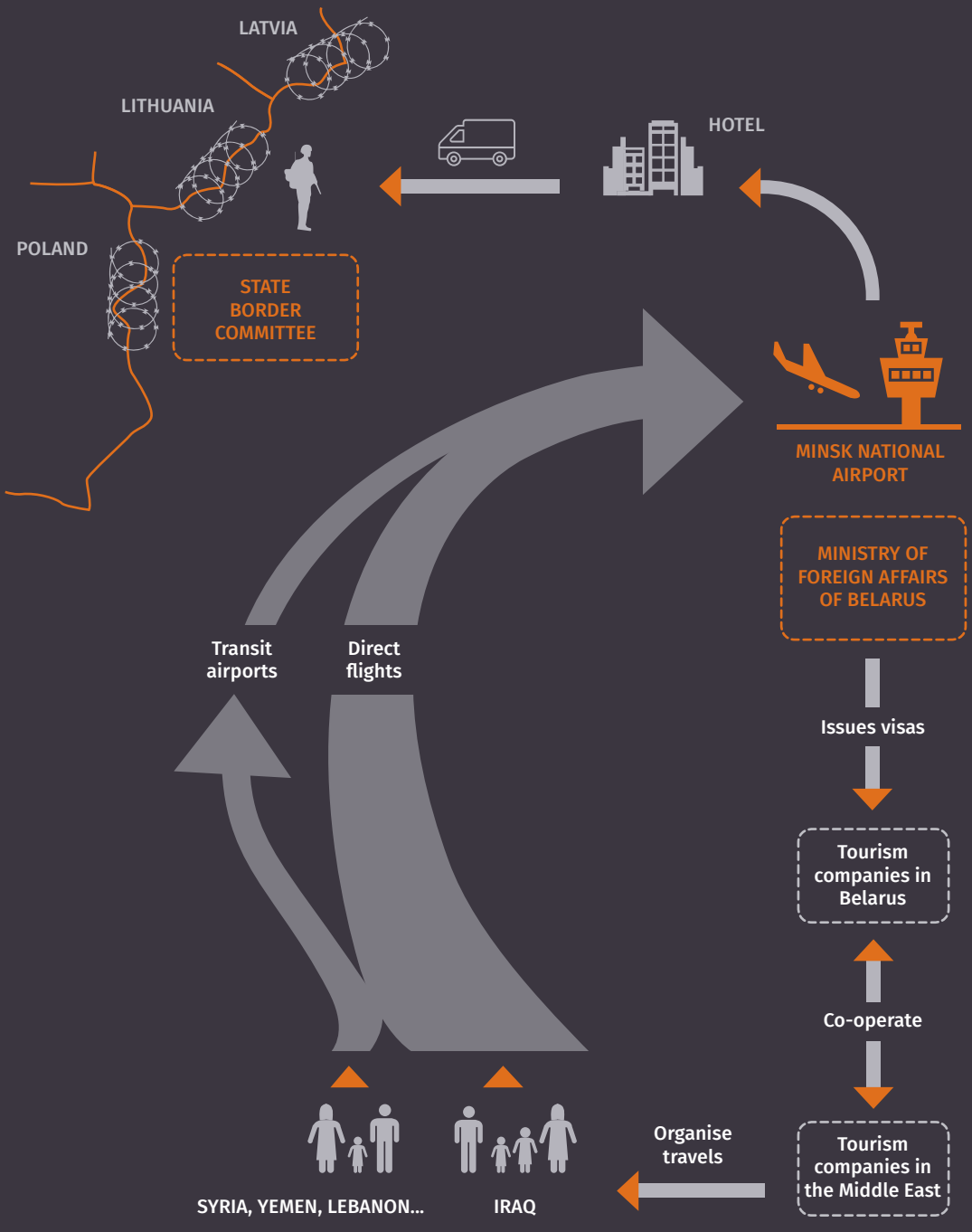
The Belarusian regime claims to have initiated legal investigations against Lithuania. It has also used international tools for legal cooperation to persecute the exiled opposition members.

Economic pressure

The Belarusian state-owned company Belneftekhim suspended the export of petroleum products via Klaipėda Seaport in 2021. It is highly likely that Lukashenka aimed to punish Lithuania and thus show his support to the Kremlin, which was interested in directing Belarusian oil products towards Russian ports and had been raising this issue in bilateral meetings for some time already.

Illegal migration

Lukashenka had encouraged illegal migration through Belarus by publicly stating that Belarus would not stop migration to the EU. Belarusian institutions and private tourism agencies were involved in the organization and facilitation of illegal migration, as well as human smugglers or even ordinary Belarusian citizens, who provided transport services to the border. Good accessibility by air made Belarus easily reachable for Iraqis and citizens of other Middle Eastern countries. Belarusian border guards became implementers of the regime's decisions: instead of protecting the state border, they facilitated illegal crossings.



CHINA

CHINA PURSUES AGRRESSIVE FOREIGN POLICY AND STRENGHTENS STRATEGIC COMPETITION WITH THE WEST

China is changing its strategic posture by turning to a more assertive foreign policy, engaging in unfair economic practices and running targeted information and disinformation campaigns to increase its global influence. Over the last year, China has significantly shifted the way it practices its diplomacy. Chinese diplomats and state officials have taken up a more nationalistic tone, they fiercely respond to any kind of international criticism directed at the Chinese Communist Party (CCP) and disseminate the CCP's narratives on foreign (social) media. China's officials actively promote the alleged advantage of the CCP's authoritarian rule over the Western democratic model of governance. Those who do not follow the CCP's ideological directives are pushed to do so by punishments and a rewards system.

China's president Xi Jinping is the chief decision maker in the Party. Highly likely, he will seek a third term in power in 2022. Foundation for Xi's reelection is already being set, demonstrated by an increased search of officials loyal to the president, the purge of potential opponents and announcement of a new historic ideological resolution of the CCP, which consolidates Xi's status and power.

China is actively engaged in global policymaking by exploiting multilateral organizations, namely the United Nations (UN). China seeks to gain influence in the organization by pushing its officials to the UN senior posts, conducting various lobbying activities and providing financial contribution to the UN missions. Coordination between China and Russia at the UN, namely the abuse of

veto power in the Security Council, adds to failure to form a coherent response from the organization. Furthermore, both countries seek to shape human rights concepts and other sets of norms to the benefit of authoritarian regimes. In 2021, China together with Russia voted against stripping Syria's voting rights at the Organization for the Prohibition of Chemical Weapons. They both voted against Poland's resolution condemning the use of chemical weapons. Being some of the biggest global spenders on space programs, China and Russia initiated joint resolutions on space legislation in favour of their developed and deployed space capabilities.

China is seeking to divide NATO and the EU so that it could set terms of communication and business on those favourable to Beijing. Through diplomatic pressure and economic tools, China undermines NATO and the EU political cohesion in dealing with Beijing. As of now, China poses no direct military threat to the Alliance, yet overlapping economic and security interests in areas of relevance to the Alliance will increase strategic challenges to NATO and the EU in the long run. China's global economic and military ambitions, its access to a wide range of cutting-edge technologies will not only have commercial and economic implications but also military ones, as they will weaken and could undermine NATO's defence technological edge and future fighting capabilities.

Beijing seeks to cooperate with Russia in the fields that are of outmost importance to China, namely on the development of 5G, cybersecurity, space and lunar research, artificial intelligence and nuclear energy. To date, mutually beneficial yet increasingly asymmetrical cooperation lets China partially offset the loss of technology sources in Western markets, also to counterbalance the U.S. strategic pressure. In 2021, China and Russia pledged to boost cooperation on a joint lunar space station, space exploration, nuclear energy, data security and defence technologies. To date, China's participation in Russia's military exercises is mostly intended to underline close military relations between the two countries.

By consolidating their technological and financial capabilities or issuing joint diplomatic statements, China and Russia seek to outweigh Western leadership. Intended China-Russia collaboration in most sensitive security fields might contribute to China's ambitions to dominate in cutting-edge technologies, thus increasing challenges and security risks for NATO in the long term.

CHINA INITIATES INTERNATIONAL GUIDELINES FOR DIGITAL GOVERNANCE

China considers data to be a strategically important tool of power in order to become the world leader in the field of emerging and disruptive technologies. The need for such data depends on the nature and purpose of technologies that are being developed, whether it is artificial intelligence (AI), the Internet of Things or any other technology. The algorithms may require video material from public surveillance cameras as well as data reflecting consumer behaviour in social media, online shopping, online search engines or smart devices. In order to ensure smooth collection and storage of data, China is proposing international data governance rules in line with its national interests.

The Global Initiative on Data Security (GIDS) proposed by China aims primarily to counter Western criticism of the unreliability of Chinese technologies, as well as to ensure the state control over flows of information and to restrict foreign interference in China's digital sovereignty, i.e. the state's rights to manage digital content, services and infrastructure.

Although the majority of the GIDS provisions seem to be similar to the data protection norms applicable in the West, they are incompatible, since China's practical information control policy is based on censorship. For example, the Great Firewall of China blocks Western online platforms, apps, websites and social networks such as Google, Facebook and Instagram.

China promotes provisions of the GIDS internationally through the Digital Silk Road initiative, but so far it has only received support from authoritarian regimes and developing countries. The Digital Silk Road, launched in 2015, is a part of China's broader Belt and Road initiative. In line with the Digital Silk Road, China provides technological support to the countries that show interest: it invests in and develops AI and mass surveillance technologies, telecommunications networks, e-commerce and other areas related to technological development and its application. In response to the economic and social consequences of the COVID-19 pandemic, China claims that this initiative will help countries to recover from the pandemic by developing technologies and creating a 'peaceful' cyberspace.

CHINA USES COERCION AGAINST COUNTRIES, WHICH, ACCORDING TO CCP, VIOLATE THE REGIME'S STRATEGIC INTERESTS

In recent years, there has been a tendency showing that China is increasingly exerting pressure on multiple countries in an attempt to change their domestic and foreign policies. China is most active in putting pressure on countries which allegedly violate the 'red lines' of its strategic policy – they establish closer ties with Taiwan, express concerns about the human rights situation or management of the pandemic in China and are taking action to limit the penetration of Chinese companies into their economic sectors of strategic importance. The CCP sees these actions as a threat to the principle of a 'one China policy', the stability of the regime and the economic development of the country. In order to adjust the behaviour of other countries, China uses various means of pressure, which, according to the experience of many countries, are implemented in a comprehensive manner.

Chinese authorities and media outlets do not shy away from using highly aggressive rhetoric to criticise policies of other countries, using terms such as "revenge", "punishment" or "counter-attack". This rhetoric is intended to deter other states from similar precedents and mobilise Chinese society to protest. In the Chinese media, decisions of states that are not in the interests of the regime are presented as being determined by other actors, mostly the US, or as ones contradicting to general political trends, for instance, policies of other countries towards China. The Chinese public is encouraged to protest in the forms available to it, i.e. to express criticism on social media, boycott the acquisition of goods, or to stop travelling to a specified state.

Aggressive public communication

In response to the visit of the President of the Senate of the Czech Republic to Taiwan in September 2020, the Chinese media announced that China would cancel direct flights and limit tourist flows to the Czech Republic.

China's aggressive rhetoric is often accompanied by measures of political pressure to show that policies that are not in China's interests face concrete consequences. By pressing other states, China tends to freeze diplomatic

relations, lower the level of diplomatic representation and impose sanctions on certain individuals.

Political pressure

In 2010, China froze diplomatic relations with Norway for six years in protest against the Nobel Prize Committee's decision to award the Nobel Peace Prize to a Chinese dissident. In 2021, China imposed sanctions on ten members of the European Parliament (EP) as a countermeasure, following restrictions by the EP on Chinese officials involved in human rights violations against Uyghurs.

China exploits economic dependence of other countries as one of the most effective means of pressure. The main objective is to create barriers in areas of trade, investment, manufacturing and business environment. Not wanting to spoil its image as a reliable partner internationally, China mostly implements economic restrictions informally, for example, by introducing additional customs controls on goods, by no longer issuing authorisations for the alleged non-compliance with sanitary requirements or by instructing its companies not to extend contracts with producers in the country concerned. The Chinese government is not obliged to formally issue economic sanctions, since the CCP units operating in Chinese companies ensure their informal implementation.

Economic constraints

In this way, in 2020, under the guise of sanitary requirements, China completely restricted beef imports from Australia, the country which at that time actively encouraged other states to pay greater attention to the investigation into the origins of COVID-19.

As a result of recent decisions taken in Lithuania concerning the withdrawal from the 17+1 cooperation format or the opening of the Taiwanese Representative Office, China uses a wide range of coercive measures against Lithuania. It implemented aggressive information campaign, applied unofficial economic restrictions, unilaterally lowered diplomatic representation level, and expanded its intelligence collection capabilities, including hostile activities in cyber space. It is highly likely that in order to deter other countries from similar decisions, China will continue to put pressure on Lithuania; however, China will officially dispute any accusations related to it in order to minimize negative outcomes to its image and potential international response.

GEOPOLITICAL SITUATION AFTER THE TALIBAN TAKEOVER OF AFGHANISTAN

Russia

Takes a pragmatic position to avoid military involvement

Seeks to ensure stability in the region and prevent the terrorism threat

Seeks to become a stabilising leader in Central Asia

Exploits the situation to criticize NATO

China

Has signaled its readiness to engage with the Taliban

Seeks economic benefits and mitigation of the terrorism threat in the region

Creates an image of a reliable partner as an alternative to the West

Iran

Shows main interest in protection of borders by stopping illegal migration and terrorism

Pakistan

Seeks to limit India's influence in Afghanistan

Has lifted border crossing restrictions

Provides Afghanistan with humanitarian aid

Mediates international discussions on the situation in Afghanistan

CONFLICT REGIONS

CONFLICT REGIONS FACE INCREASING ISOLATION FOLLOWING COUP D'ETATS

In 2021, the worst-case scenario came to fruition in Afghanistan. As the Taliban continued an armed struggle and maintained its hardline position regarding internal peace negotiations, the security situation deteriorated. Meanwhile, political divisions plagued the government camp. Following the announcement of the withdrawal of US and NATO forces, the Taliban intensified its offensive in most provinces and finally took over the country in August. Although the Taliban's return to power was anticipated, such a swift victory was unexpected.

In many places of the country, the Taliban came to an agreement with local senior political and military figures, which enabled fighters to advance quickly, often without a resistance from the Afghanistan security forces (ASF). Problems were exacerbated by soldiers' tendency to hold a strong sense of loyalty to their kin and tribe but no obligation to defend the state. In addition, systemic issues in the ASF, such as corruption, the so-called ghost soldiers (non-existing troops added to lists by officials who pocketed their wages so), frequent casualties, low morale and a lack of trust in political leadership of the country contributed to giving up resistance and the Taliban's swift victory.

Taliban fighters had been highly motivated by the forthcoming victory, especially since the bilateral US-Taliban agreement, signed in 2020. The Taliban's main goal had always been a withdrawal of foreign forces from Afghanistan and restoration of the Islamic Emirate. The Taliban negotiated a release of their detained fighters and kept expanding its influence in rural areas. Moreover, the Taliban was successful in spreading a narrative of military power and

upcoming victory in the information sphere, encouraging the ASF personnel to surrender by promising amnesty and financial rewards in return to them.

The collapse of democratic government caused chaos in the capital and prompted an urgent evacuation campaign. Over the course of two weeks, foreign nations managed to airlift more than 120,000 foreign citizens and vulnerable Afghans abroad. At the same time, the Taliban declared the restoration of the Islamic Emirate of Afghanistan and imposed harsh restrictions based on Sharia law. Public statements of Taliban leaders regarding human rights, freedom of press and promised amnesty for government officials proved just a rhetoric for a better image of the Taliban in the eyes of international community but not a genuine objective. In reality, radical Taliban views have not changed fundamentally.

The deteriorating economic situation in Afghanistan is the reason for increasing poverty and it poses a risk of humanitarian crisis, which could result in migration of millions of Afghan citizens to the neighbouring countries and, likely, to the European Union. In order to avert a complete collapse of the economy, the Taliban will seek to maintain a constructive dialogue with foreign countries and avoid international isolation in order to gain financial support, which Afghanistan is heavily dependent on.

Lithuanian military evacuate civilians from Afghanistan

Throughout 2021, the security situation in Syria, Libya and Iraq remained relatively stable and currently there are no indications that it could significantly deteriorate in the near term. In the Sahel region, extremist groups are expanding their areas of activity in Mali, Burkina Faso and Niger, recruiting new members and entrenching themselves in local communities, while operations of international military forces bring only short-term effects. It is almost certain that in the long term the lack of rule of law and security vacuum will persist.

Military junta in Mali is desperately seeking to stay in power. To this end, it is collaborating with Moscow. Contractors from the Russian private military company Wagner already operate in Mali. Involvement of Wagner in Mali (a similar model is used in Syria and Central African Republic) will likely jeopardize relations between the government of Mali and its Western partners, who could reconsider their military support and participation in international operations in the country.

THE ACTIVITY OF HOSTILE INTELLIGENCE AND SECURITY SERVICES

RUSSIAN INTELLIGENCE SERVICES POSE A THREAT TO LITHUANIAN NATIONAL SECURITY BY ACTING FROM FOREIGN COUNTRIES

Russian intelligence services (RIS) remain a major intelligence threat to Lithuanian national security. Russia maintains significant intelligence capabilities against foreign states. All RIS – the Foreign Intelligence Service of the Russian Federation (SVR), the Federal Security Service (FSB) and the Main Directorate of the Armed Forces General Staff (GRU) – collect intelligence and counterintelligence information.

By collecting intelligence information related to Lithuania and conducting influence operations at peacetime, RIS seek to impact the state's political processes and defensive capabilities in the long term. An additional threat emerges from the continued close cooperation between Russian and Belarusian intelligence services against Lithuanian interests and joint collection of information necessary for military planning.

Although the COVID-19 pandemic and related restrictions have not changed Russian strategic foreign policy goals, they partly restrict Russian intelligence capabilities in foreign states. Russian HUMINT activity from the territory is constrained due to COVID-19 restrictions, but travelling allowed to Russian or Belarusian territory remains an intelligence threat to Lithuanian residents.

Intelligence from the territory is a HUMINT activity, when recruitment of a potential agent is conducted in Russian or Belarusian territory. Further handling might be organized in a third country.

Traditionally, RIS have been most active against Lithuania from the Russian territory. People who regularly travel to Russia or Belarus remain among the main recruitment targets for RIS. When selecting a potential agent, both access to information and personal motivation to cooperate play significant parts. The priority is given to the people who have links with Russia or Belarus and are ideologically motivated – actively or tacitly support Russian and Belarusian policies and may already have build ideological loyalty. Therefore, individuals without access to classified information or any other high ranking position are still on the radar as potential recruits.

On 12 November 2021, the Klaipėda Regional Court found Lithuanian citizens Mindaugas Tunikaitis and Aleksėjus Greičius guilty for spying. The court stated that these individuals had been recruited by the Russian FSB and performed its tasks. Tunikaitis, living in the border town, regularly monitored, photographed and filmed various border facilities and activities for remuneration as well as performed other FSB assigned tasks. In cooperation with the Russian FSB official, Greičius organised events financed in whole or in part by the FSB, photographed the individuals involved, gathered intelligence and performed other tasks. These cases of espionage confirm that Russian intelligence services also recruit those Lithuanian citizens who do not have access to classified information.

Lithuanian intelligence agencies have been observing GRU attempts to establish a network of agents, tasked not only to collect information on Lithuanian Army infrastructure and other strategic objects but also to provide operational support to other GRU activities in foreign states.

Personal characteristics of a person that might attract interest of hostile intelligence services

RUSSIAN AND BELARUSIAN INTELLIGENCE TARGETS – OPPOSITION ACTIVISTS WHO MOVED TO LITHUANIA

The ruling regimes in Russia and Belarus are increasing their pressure on non-systemic opposition organisations, which, due to strong government and law enforcement pressure and persecution, are shifting their activities to foreign states. These states attract the attention of Russian and Belarusian law enforcement agencies, propaganda journalists and intelligence services.

Russian intelligence services, especially the Russian FSB, are active against opposition organisations and activists both within Russia's territory and abroad. The main unit of Russian intelligence services working against Russian opposition activists is the Directorate for the Protection of Constitutional Order of the FSB's Service for Protection of Constitutional Order and Counter-Terrorism. It is responsible for overseeing and controlling political, social, religious, extremist organisations and processes in Russia. FSB officers carry out surveillance of opposition activists, wiretap them, seek to infiltrate their surroundings, organise provocations and even attempts upon their lives. In 2020, FSB officers from this unit organised an attempt to assassinate Russian opposition leader Navalny.

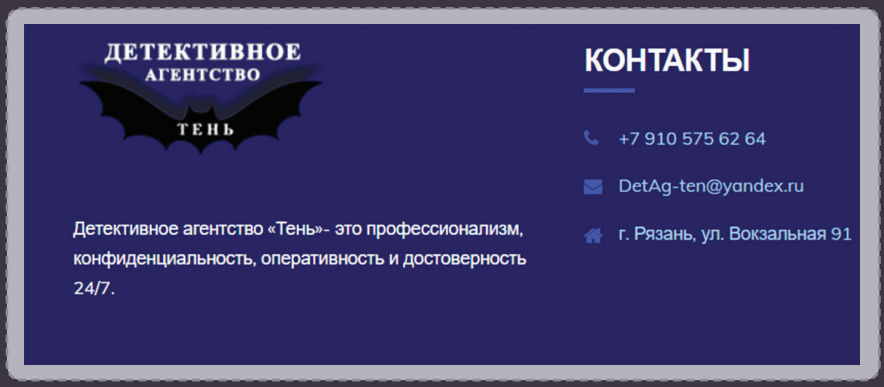
Lithuania is one of the main directions of emigration for Russian opposition activists. There are several hundred Russian citizens who have been granted asylum in Lithuania, as well as individuals who did not apply for special status but are engaged in political or journalistic activities. Representatives of political, public and media organisations opposing the Russian government from Russia or EU countries regularly visit Lithuania; Russia's opposition events take place here as well.

WHILE VISITING LITHUANIA NAVALNY WAS UNDER SURVEILLANCE BY FOUR RUSSIAN CITIZENS

Russian leadership and intelligence services consider Navalny and his organization as posing high-risk to the regime. For this reason, Navalny was under surveillance both in Russia and abroad even before his attempted assassination. Our intelligence suggests that during Navalny's visit in Lithuania in April and September 2019, a group of four Russian citizens followed him from Russia with a task to carry out his physical surveillance. This group of people made simultaneous visits across Europe as Navalny. These Russian citizens officially claimed to be retired and stated tourism as the purpose of their trips to Europe. All of them are affiliated with Ten (Тень), a private detectives' agency, based in Ryazan (Russia), and were previously employed in Russian law enforcement or military. Russian intelligence services frequently use various intermediaries – people, companies or organizations – indirectly related to them in order to minimize possible risks in case of mission failure.

In recent years, intelligence services of Lithuania's allies have uncovered a number of attempted assassinations for opposing or displeasing the Kremlin that Russian intelligence planned and perpetrated. The disclosed operations reveal that Russia's political leadership and intelligence services consider the risk of possible response for conducting such operations abroad as acceptable.

Russian citizens who carried out Navalny's surveillance across Europe: Alexandr Borzunov (b. 1976), Vyacheslav Romashin (b. 1973), Andrey Malikov (b. 1977), Alexandr Zarubin (b. 1982)



Russian intelligence services are interested in information about the Russian opposition activists residing in Lithuania and their organisations, plans and courses of action. RIS may seek to infiltrate agents into Russian opposition organisations operating in Lithuania, deploy intelligence staff with unconventional cover, and to penetrate the IT systems of opposition activists and organisations by cyber means. As political repression in Russia is expanding and the number of political émigrés from Russia is growing, the attention of Russian intelligence services to the opposition activists in Lithuania is also likely to increase.

Since the beginning of the political crisis in Belarus, when Lithuania became one of the centres for Belarusian political opposition, the activity of Belarusian intelligence services against Lithuania has increased. Belarusian intelligence services are involved in handling the political crisis in Belarus. They seek to identify and intimidate the opposition and its supporters, besides, they use the collected intelligence for discrediting them and running propaganda campaigns against them. Belarusian intelligence services are not limited to intelligence gathering and act aggressively against opponents of the Belarusian regime in Belarus and abroad. It is highly likely that Belarusian intelligence services planned and carried out the diversion of Ryanair's aircraft flying from Athens to Vilnius, to forcefully land in Minsk airport in order to detain Roman Protasevich, who resided in Lithuania.

The State Security Committee (KGB) of Belarus monitors the activists of Belarusian opposition living in Lithuania, gathers information about them, records their activities and seeks leverage to influence them. Not only the KGB but also the services subordinate to the Ministry of the Interior of Belarus (e.g. GUBOPIK, the Main Directorate for Combating Organised Crime and Corruption) and the Main Intelligence Directorate of the General Staff of the Armed Forces of Belarus (Belarusian GRU) are using active measures against the opposition. In addition, Belarusian intelligence services work against the political opposition in cooperation with their Russian counterparts.

It is highly likely that in the near term the intelligence and disruptive activities of Belarusian intelligence services against the country's political opposition and diaspora will intensify, while foreign states, the opposition from which is most active, will remain targets for propaganda, discrediting and disinformation campaigns.

BELARUSIAN COMINT CAPABILITIES ENABLE TO COLLECT A WIDE RANGE OF INFORMATION ABOUT LITHUANIA

Last year, Belarusian border guards were actively involved in coordination of illegal migrant flows. Belarusian border guards were taking pictures and videos of Lithuanian border surveillance systems; on a regular basis they turned a blind eye to migrants present at the Belarusian border zone and often facilitated their crossing into Lithuania.

Belarus actively used COMINT against Lithuanian soldiers and Sate Border Guard Service officers, guarding the Lithuanian-Belarusian border. According to the available information, their mobile communications metadata was intercepted and later used for influence operations. In addition, information from social media networks was used for identifying Lithuanian officers working at the border zone with Belarus in order to send threatening messages from fake accounts to them.

Belarusian intelligence also collects information on infrastructure important to Lithuanian national security, Lithuanian border area, border security systems and border vulnerabilities in general. Such information is likely used not only to direct illegal migrants but also for Belarusian and Russian military planning.

LEGAL REGULATION STRENGTHENS THE ACCOUNTABILITY OF CHINESE COMPANIES TO THE COUNTRY'S INTELLIGENCE SERVICES

The Chinese government is consistently improving the legislative framework governing intelligence and security services, which not only determines the functions of China's intelligence but also refers to their relationship with other entities. In accordance with these laws, a hypothetical Chinese company active in fields of social media, technology and telecommunications should:

Counter-Espionage Law (2014)	support counter-espionage activities of intelligence and security services in China and beyond, provide access to the company's electronic communications resources and facilities
National Security Law (2015)	provide recommendations to help the services carry out information gathering tasks and, in the event of a threat to national security, mobilise the company's employees to prevent that threat
Counter-Terrorism Law (2015)	inform intelligence and security services about the location of Uyghur, Tibetans and other people suspected of terrorism in China, assist in decoding of their telecommunications and interception of communication signals
Cybersecurity Law (2016)	provide technical support to the services, control the data flows of the company's social media platform by identifying ideas questioning China's sovereignty and socialist system and defamatory statements
Intelligence Law (2017)	provide cover for intelligence officers in China and beyond, allow them to access all the company's data, information systems and media
Anti-Espionage Regulation (2021)	organise preventive training for staff travelling abroad. Conduct intelligence surveys on their return; they would be carried out by the company's division responsible for implementing counter-intelligence measures

CYBER SECURITY

STATE ACTORS AND THEIR AFFILIATES EXPLOIT A WIDE RANGE OF TOOLS FOR HOSTILE CYBER ACTIVITY

Hacker groups coordinated by adversarial states remain the primary threat to security of information systems of Lithuanian institutions and organizations. There is an obvious correlation between major international political developments and hostile cyber activities targeting Lithuanian entities. These trends are particularly visible when adversarial states consider our national decisions to be running against their interest or reputation.

In Lithuanian information networks Russia-attributed cyber espionage groups are the most active comparing to other state-affiliated cyber actors. This is also a worldwide trend: Microsoft announced that from July 2020 to July 2021 Russia had been responsible for 58 percent of all the detected state-sponsored cyber-attacks. The US, Ukraine and NATO nations are considered the primary targets of Russian cyber actors.

State cyber actors primarily aim at establishing a long-term access to information systems in order to have a continuous capability to collect specific information on military and political matters. The hackers not only collect data from the system they have compromised but also search for ways to get access to classified information, they analyze the system's architecture. While implementing this task, they try to get access to the targeted (usually state institution) networks undetected and create persistent mechanisms that allow espionage groups to access the system even if a malicious code is detected and partially removed.

Over the recent years, espionage groups, traditionally known for their clandestine activity, have been used for more public operations – leaking of hacked

information or destructive incidents. On certain occasions the information hacked is placed into a specific context or is mixed with fake information in order to discredit a person or organization, influence society's opinion in favour of Russia. Another type - destructive attacks - aim to disturb or disrupt operation of critical infrastructure. Such Russian activity is detected in multiple states, including Lithuania.

During *ransomware* attacks the targeted information system's data is encrypted and ransom is requested for the recovery of information.

In order to sabotage the opponents' information systems or disguise traces of malicious activity, state-affiliated cyber actors also conduct *ransomware* attacks, which are typical of criminal hackers. In 2021, the US, UK and Australian cyber security agencies attributed the use of a hard disc encryption and security program BitLocker against transport and health care sectors and other organizations to the Iranian government-supported hackers. The growing number of *ransomware* attacks and their use by state-affiliated actors make the attribution more complicated.

RIS-related cyber actors not only use the tools associated with the criminal world but also cooperate with criminal hackers. Some of the criminal hackers provide *ransomware-as-a-service*. Clients of such service get access to cyber infrastructure and tools, which enable them to conduct automatic data encryption. Such scheme further complicates the attribution. One of the examples of such activity possibly is a vast scale *ransomware* attack against the US oil product operator Colonian Pipeline and Japanese IT company Toshiba Tec Corporation unit in Europe, which were carried out by the group *DarkSide* in 2021.

It cannot be ruled out that some of the major attacks initially attributed to the criminal world have been carried out in an interest of an adversarial states. Some of the hackers without any known links to any adversarial state have acquired such (destructive) capabilities that they can pose a threat to national security due to the scale of attacks or their chosen targets. In 2021, Russia-linked Conti group of criminal hackers attacked various state services including the police, emergency medical aid and health care service organizations, whose IT system malfunction could have had effects on people's lives. Russia-associated hacker groups that provide a *ransomware* service have been exclusively attacking targets outside CIS countries.

Ransomware and other type of cyber-attacks often make an impact not only on the initial targets but also on the organizations further down the supply chain. Since organizations transfer an increasingly larger and more significant part of their activities to electronic space, and data storage as well as other services are outsourced to other companies, data security, financial situation or even ability to operate now more than ever depend on various service providers. During supply chain attacks hackers choose the most vulnerable elements – smaller suppliers or companies with insufficient cyber security – as their initial targets. Supply chain attacks that might affect the strategic infrastructure are assessed as a potential threat to Lithuanian national security. Major r*ansomware* attacks conducted against other states may have trans-border effects and disrupt organizations in Lithuania or any other state.

Examples of supply chain attacks in 2021 attributed to state cyber actors

- **The French national cyber security agency publicly accused Russia GRU-linked Sandworm group of attacks against networks of French organizations from 2017 to 2020. The group gained access to target systems using vulnerabilities in software sold by a local IT company.**
- **RIS-linked group APT29, which in 2019 and 2020 conducted a large-scale attack/ large scale attacks against the IT management software provider SolarWinds and its clients, started a new campaign of supply chain attacks. Likely, the companies providing IT solutions were chosen as their initial targets for the new attacks due to access to their clients' information systems.**
- **The attacks by Lazarus group attributed to North Korea were made public after the group conducted malicious activity using software of South Korean and Latvian IT companies.**

As the distinction between malicious activities employed by state and non-state cyber actors and tools is gradually blurring, and as the integration of information systems of various organizations is growing, the attractiveness for various adversarial states to use cyber means for subversive and espionage activities will highly likely increase in the near term. In the long term, various state institutions and related organizations will highly likely be among major targets for state-sponsored cyber groups.

INTENSIVE EXPANSION OF CHINA'S CYBER ESPIONAGE CAPABILITIES THREATENS THE SECURITY OF DEMOCRATIC STATES

The aspiration of the Chinese Communist regime to dominate the world in political, military, economic and technological spheres undoubtedly promotes intensive development of the country's cyber intelligence capabilities, which complement to traditional intelligence gathering techniques. This development is seen by many Western countries as a complex and permanent threat to national security. China is increasingly using its cyber capabilities against Lithuania.

China's sophisticated cyber espionage groups collect sensitive political, military and commercial information under the direction of Chinese intelligence services. They target foreign governments, research centres, and technology and telecommunications companies. The activities of cyber espionage groups in China are coordinated by two main services – the Ministry of State Security and the Military Intelligence Department. They not only shape intelligence tasks but also enable cyber espionage groups to commit cybercrime unrestrictedly.

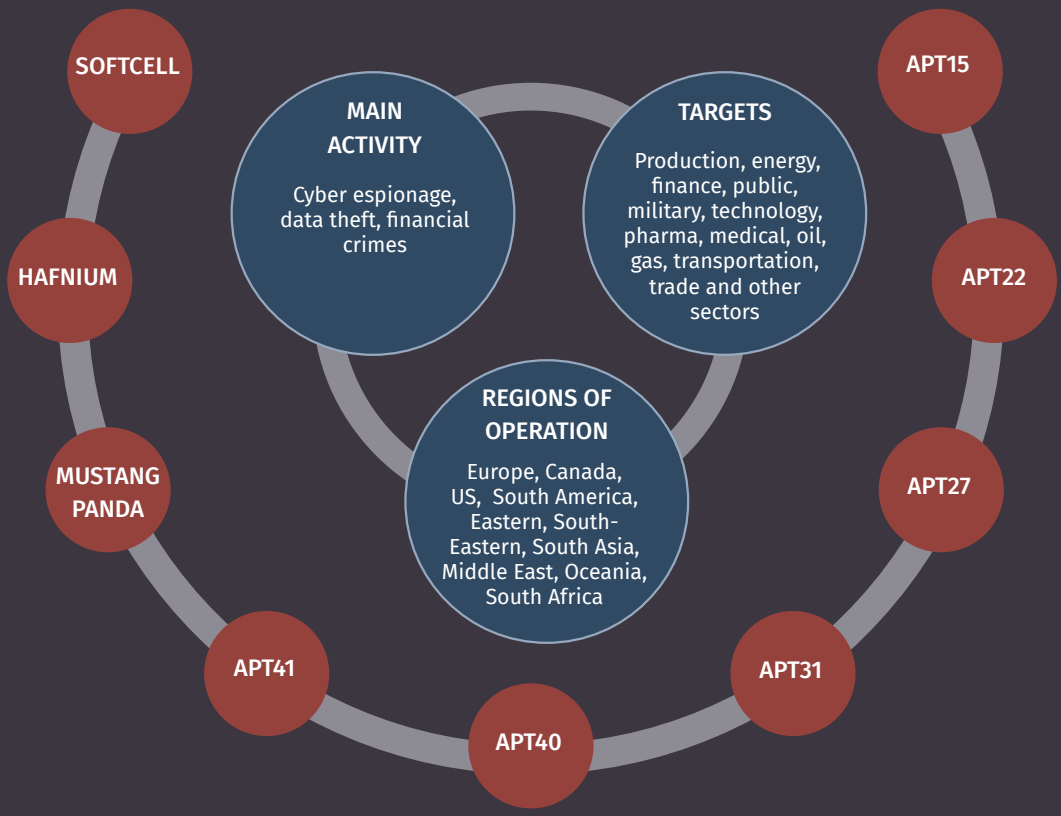
China is consistently increasing capacities of cyber espionage groups, expanding the network of their cover organisations and improving operational methods. The country's universities, private IT companies, freelance IT experts and cybercriminals are involved in the implementation of cyber intelligence objectives. China demonstrates its high level cyber capabilities by developing sophisticated and advanced malicious system control software tools.

In 2021, state sponsored China's cyber espionage groups carried out a large-scale cyber operation against Microsoft, one of the largest IT companies in the world. HAFNIUM, a group with ties to Chinese intelligence services, detected and exploited currently still unknown vulnerabilities in the email system, MS Exchange. This allowed Chinese intelligence to take over a large amount of data from Microsoft's clients around the world.

MAIN GROUPS SUPPORTED BY CHINESE INTELLIGENCE SERVICES

MINISTRY OF STATE SECURITY (MSS)

MILITARY INTELLIGENCE DIRECTORATE (MID)



GHOSTWRITER ACCELERATES ITS CAMPAIGN

At least 11 cyber-enabled information attacks carried out in the Lithuanian information space in 2021 are considered a continuation of previously observed hostile activity and associated with Ghostwriter. Historically the group primarily targeted NATO and the national defence system, but recently it has also tried to exploit the migration crisis and the pandemic. In addition, a growing part of the disinformation spread during the attacks was related to Belarus, including the migration crisis, NATO activity in the region and the Belarusian opposition abroad. Perpetrators likely expanded the scope of topics with an intent to influence a wider part of society and make a larger impact.

Despite the limited impact of disinformation on Lithuanian institutions and society, perpetrators use a wide spectrum of measures to spread the news contradicting the state interests. The imitation of state institutions and media websites and (or) hacking them in order to change their content, spoofing e-mail sender information, hacking social network accounts are all actively used by perpetrators. Spoofed email or social media accounts (e.g. allegedly used by politicians) are used in order to increase the spread of disinformation and enhance its credibility. The executers of Ghostwriter campaign are also likely looking for other methods to increase the effectiveness of their malicious activity.

INFORMATION SECURITY

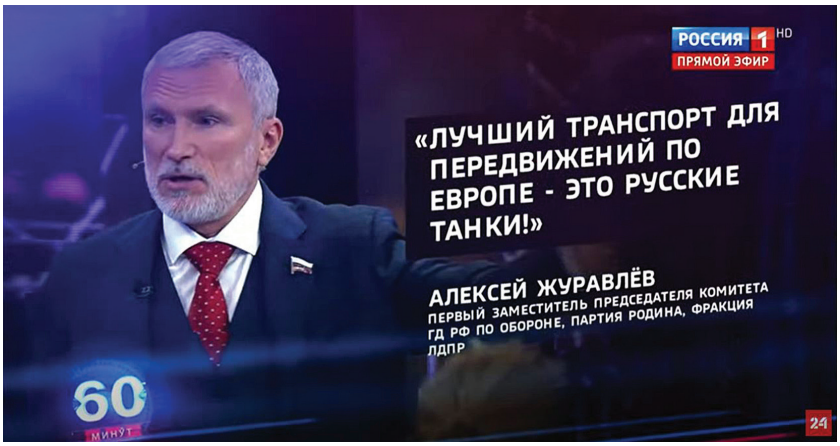
RUSSIAN AND BELARUSIAN PROPAGANDA CAMPAIGNERS INTENSIFIED THEIR ACTIVITY AGAINST LITHUANIA

During the outbreak of the COVID-19 pandemic the number of visits by Russian propagandists to Lithuania temporarily decreased. Recently, Russian propaganda media representatives residing in Russia and EU countries renewed their visits to Lithuania and gather material again. The number of Belarusian propaganda attempts to obtain materials for their production in Lithuania is also increasing.

A large-scale Russian and Belarusian propaganda campaign against Lithuania, Poland and other countries in the region was organised in the wake of Lukashenka's instigated migration crisis. This propaganda campaign could compare to Russia's continued smear campaign against Ukraine in terms of intensity, aggressiveness and volume of fake news.

Fake news from Russian and Belarusian propagandists related to the migration crisis is unsophisticated, designed to arouse negative emotions quickly and are easy to rebut. A typical example of such falsification is the presentation of video material with personnel of the Belarusian forces using firearms to frighten migrants and posing the former as officials of the military or law enforcement agencies of other states. Russian and Belarusian propaganda production on the topic of the migration crisis is characterised by war and hate rhetoric, which was abundant not only in the statements of propagandists themselves but also by the interviewed officials of the regimes.

During the migration crisis, Belarusian propaganda co-opted some of the marginal Lithuanian political radicals, who had previously often provided their commentary for Russian propaganda. It is highly likely that Belarusian propagandists contacted at least some of them on the recommendations of their Russian counterparts. This reflects a closer cooperation between Russian and Belarusian propaganda apparatuses on topics of mutual interest.



The production of Russian propagandists contained rhetoric inciting war and hatred

Russian propaganda is always interested in large-scale protests in Western countries, which they try to present as a proof of collapse of democratic order. The protest events taking place in Lithuania were not an exception; they received a lot of attention not only from Russian but also from Belarusian propaganda media. In 2021, after a long period, several large-scale protests took place in Lithuania, involving from 5 to 15 thousand people. The majority of them were peaceful citizens exercising their constitutional rights to express opinion and attend public gatherings. However, the events also attracted those promoting extremist ideologies and destructive conspiracy theories, those holding anti-constitutional attitudes and considering violence as a tool to achieve their goals, and those in support of the Kremlin's geopolitical objectives. Due to this, several small incidents occurred during the protests with one event turning into a riot. It received high-profile media coverage by Russian and Belarusian TV channels with the largest audiences. They also used footage from local political radicals and other participants who captured the turmoil and demonstratively broadcast insults directed at law-enforcement and other authorities.

In the near term, Russia plans to strengthen its propaganda eco-system in foreign countries and focus on younger Russian-speakers abroad with an intent to offer them journalism studies in Russia as well as courses, seminars and other trainings.

FSB INFLUENCES THE CONTENT OF WEB PORTALS MANAGED BY PRO-KREMLIN POLITICAL MARGINALS IN LITHUANIA

FSB → Intermediaries → Information resources in Lithuania

Not only Russian media or pro-Kremlin public figures but also Russian intelligence services conduct propaganda campaigns against Lithuania and other Western states. The intelligence services secretly disseminate propaganda in foreign information platforms – websites, social media and the press.

For several years, the FSB has been carrying out such activities directed against Lithuania by placing propaganda articles in media outlets operating in Lithuania. In doing so, FSB officers seek to disguise their links with the distributed production thus passing their pre-produced articles through the trusted intermediaries.

The articles prepared by the FSB are usually published in online media outlets – for instance, in websites *laisvaslaikrastis.lt, bukimevieningi.lt* and others – managed by pro-Kremlin political radicals or those engaged in spreading conspiracy theories. They also appear in local Lithuanian media, especially sub-national and municipal level media outlets or those with the Russian-speaking audience. The quality of such articles is usually low, they leave multiple editorial and language mistakes. The articles are signed by non-existent authors.

laisvas

Tik **2,08 eur** mėnesiui!

Vedamasis COVID-19 Aktualijos Žurnalistiniai tyrimai Mafijinė teisėsauga Politika Nuomonės Archyvas Kontaktai Facebook

«Vakcinų karas»

Šiuo metu Europoje vyksta tikra dezinformacijos kampanija apie tariamai neigiamą vakcinos Sputnik V poveikį, daeita ir iki teiginių, neva nuo šios vakcijos net miršta.

„Kryžiaus žygį" prieš rusišką vakciną pradėjo interneto portalas EUobserver, kurio centras randasi Briuselyje, o portalo finansavimas jau seniai kelia dideles abejones dėl galimai neskaidrios įtakos. Ši belgiška žiniasklaidos priemonė pranešė „sensaciją" apie mirtis-neva keturi Rusijos piliečiai mirė po to, kai buvo paskiepyti vakcina Sputnik V. Pravartu pastebėti, jog portalas rėmėsi anonominiu šaltiniu, taigi faktiškai nenurodė tikrų faktų.

Įdomu pastebėti, kad Rusijos atstovai dar prieš keletą savaičių įspėjo įvairias pasaulio žiniasklaidos priemones apie tai, kad rengiama prieš Sputnik V nukreipta informacinė kampanija, kurios pagrinis tikslas : „formuoti neigiamą požiūrį į Rusijos moksliniinkų sukurtus preparatus, kurie naudojami koronaviruso infekcijos neutralizavimui". Kaip teigė šaltinis iš Kremliaus , šios informacinės kampanijos organizatoriai savo tezes apie „pavojingą" Sputnik V vakciną stengsis pagristi tuo, kad „nuo šio preparato masiškai miršta juo paskiepyti žmonės".

In 2021, the article "Vaccine war", published in an online news media portal *laisvaslaikrastis.lt* by the order of the FSB, expressed dissatisfaction with the EU mistrust towards Russian COVID-19 vaccine 'Sputnik V'.

In Lithuania, the FSB not only distributed articles favourable to Russia but also created Lithuanian online propaganda outlets. Tunikaitis, a Lithuanian citizen who was found guilty of espionage, was ordered by the FSB, among other tasks, to administer the website *nepriklausomizurnalistai.eu*, which disseminated news in Lithuanian. After his detention, the website stopped its activity.

TERRORISM AND MIGRATION

LITHUANIA REMAINS AT RISK OF RIGHT-WING EXTREMIST TERRORIST ATTACK

There are several dozen people spreading right-wing extremist accelerationism ideology in Lithuania's digital communication platforms. Some of them began to spread their ideological views in public places and during protest action, for instance, by putting stickers and distributing flyers. The most active accelerationism supporters are aiming to radicalise teenagers and encourage the already radicalised individuals to switch from online discussions to real life actions.

Right-wing extremists also tried to take advantage of the migration crisis. However, several of their initiatives to conduct border patrols were interrupted at the initial stages. The organisers intended to locate individuals who had crossed the border and use violence against them. In addition, there were prompts to go to the Lithuanian-Belarusian border in information sources used by right-wing extremists in some European countries.

Right-wing extremists in Lithuania disseminate propaganda that incites hatred

facebook.com

Lithuanian right-wing extremist discussion groups disseminate instructions on the improvised incendiary devices or weapons, literature on martial arts and war tactics as well as manifestations of right-wing extremists who committed large-scale terrorist attacks. Such trends show that right-wing extremist activities remain a risk factor to the state security; it is possible that in the near term there might be attempts to commit a terrorist attack against ethnic or religious minorities, refugees, human rights defenders or activists.

FLOW OF ILLEGAL MIGRATION FROM BELARUS POSES RISKS TO THE SECURITY OF LITHUANIA

More than a dozen of individuals suspected of links to terrorism have used illegal migration route via Belarus, which was facilitated by Minsk regime, and entered Lithuania. Some of them concealed their ties with terrorist or extremist organisations; some were identified as having acquired military experience in paramilitary groups.

The majority of migrants crossing the border from Belarus were from Iraq. Terrorist and extremist organisations, such as the Islamic State (ISIL), the Kurdistan Workers' Party (PKK) and the paramilitary Shiite groups conducting attacks against NATO forces are active in Iraq. Some of the migrants who applied for asylum in Lithuania presented themselves as nationals of high-risk terrorism countries, namely, Syria, Afghanistan, Nigeria, Pakistan, Mali, Somalia and Yemen, as well as coming from the North Caucasus region. A large number of migrants entering Lithuania did not submit any identity documents. Some presented themselves under false names, which complicated their identification and verification and subsequently made the efforts to identify possible threats to the state security more challenging. It is also possible that among the migrants there were individuals seeking to avoid prosecution for crimes committed in their countries of origin.

For the vast majority of migrants, who illegally crossed the border from Belarus, Lithuania was a transit country on their way to reach Western Europe. Despite the increased illegal migration flows, Lithuania is unlikely to become a major target for Islamist terrorist organisations. Nevertheless, in case Belarus continues to organise illegal migration flow from conflict regions to Europe's eastern borders, it is likely that members of terrorist or extremist organisations will try to use it more actively; therefore the risk of possible terrorist use of transit route through Lithuania would increase. In the near term, radicalisation of individual migrants is possible. The main risk factors are susceptibility to terrorist propaganda and failure to obtain asylum or settle in Lithuania or another EU Member State.

DURING THE MIGRANTS' SCREENING PROCESS, LITHUANIAN INTELLIGENCE HAS IDENTIFIED A DOZEN INDIVIDUALS SUSPECTED OF TIES WITH TERRORIST ORGANISATIONS AND PARAMILITARY GROUPS

Individuals with links to EU–designated terrorist organisations

The individual who entered Lithuania introduced himself by the previously held identity, concealed his ties with terrorist organisations and the fact of visiting the conflict zone. It was established that the individual travelled to conflict regions with the purpose to fight on the ISIL side. As a result of the collected information intelligence, the asylum was not granted.

Individuals involved in the activities of paramilitary groups

The individual concealed his ties with a paramilitary group, weapon skills and military experience in conflict regions. As a result of discovering this information, the asylum was not granted.

THREAT OF TERRORIST ATTACKS TO EU COUNTRIES WILL REMAIN HIGH

Radical Islamists committed far fewer attacks in Europe last year than in previous years. Individuals motivated by Islamist extremist ideologies were responsible for five attacks in Germany, France, Norway and the United Kingdom, but no direct contacts between perpetrators and terrorist organisations have been detected. European intelligence and law enforcement services prevented a number of extremist attacks. During the year, several violent acts with features of a terrorist attack took place in Europe, but their motivation was unclear and the mental health status of suspects was questioned.

Currently, ISIL in Syria and Iraq does not have the capacity to organise terrorist attacks in Europe, but it is actively spreading terrorist propaganda to encourage radicalised individuals to act in Europe on their behalf. COVID-19 restrictions on public life in Europe pose a risk of self-radicalisation of some individuals. Social isolation and the lack of social contacts are partly responsible for an increased encounter with radical ideologies online, leading to the attempts by radicalized individuals to reach out to propaganda disseminators and engage in extremist activities. Thus, in the near term, a direct threat of terrorist attacks in Europe will be posed by radicalised individuals, who are not directly linked to terrorist organisations and who can carry out simple tactic attacks with own capabilities and resources directly available to them.

Police officers are more frequently becoming terrorists' targets in Europe. Honouring the police employee, a victim of the terror attack in Rambouillet, a suburb of Paris, 2021.

AFP / Scanpix

The probability of a terrorist attack in Lithuania is low

- **No organised groups of supporters of Islamist and political extremism in Lithuania have been identified**
- **Lithuania has not been threatened by terrorist acts from abroad**
- **Foreigners identified in the illegal migration flow from Belarus, suspected of having links with terrorist or paramilitary organisations, have no intention to act against Lithuania, their movement is restricted**
- **There are no signs of increasing radicalisation in Lithuania**
- **Due to the impact of online extremist propaganda, some individuals are exposed to the risk of radicalisation**

ECONOMIC AND ENERGY SECURITY

BELARUS AND ROSATOM CONTINUE OPERATION OF THE BELARUSIAN NUCLEAR POWER PLANT DESPITE NUMEROUS RECURRING DESIGN AND ENGINEERING DEFECTS

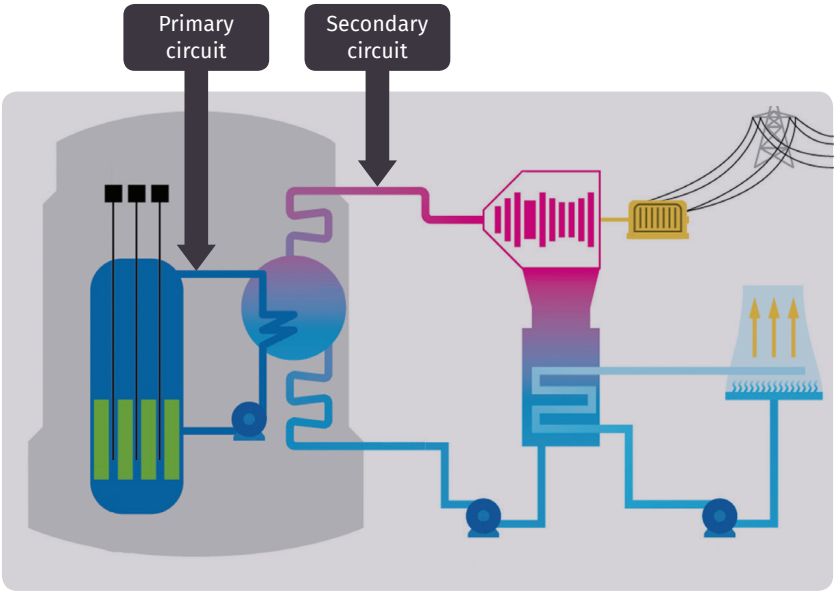
The Russian nuclear power corporation Rosatom presents the Belarusian nuclear power plant (NPP) as a success story and based on this project intends to expand the use of its technologies and gain influence in other countries. On 10 June 2021, Alexei Likhachev, CEO of Rosatom, announced the commercial launch of the Belarusian NPP Unit 1 and was delighted with the 'historic event'. He claimed it to be the result of "a large amount of work done by a team of highly qualified specialists from both countries".

Public rhetoric, praises for the project and new technological solutions do not reflect the real situation in the NPP. Frequent disconnections from the network indicate that the engineers constantly struggle with equipment defects and have to address the recurrent malfunctions with temporary solutions to keep the NPP systems running.

Moreover, the Belarusian NPP has defects in Rosatom installed systems, which are crucial to nuclear safety. One of the core systems – primary cooling circuit, which contains water heated by nuclear fuel rods and transfers heat from the reactor core, had technical issues (was not leak-proof) even before the start of its commercial operation . While Unit 1 was working at the capacity of 100%, it was decided to conduct an emergency shut down test. However, an incident occurred. It was identified, that the system of the primary circuit had a leak. Contaminated water, which circulates in the primary circuit, leaked to

The principle of operation of VVER reactors is based on a system of two separate circuits. Water in the primary circuit flows through the core of the reactor and heats itself up while cooling it, but does not boil due to its high pressure. As water flows through the reactor core, it is contaminated with radioactive substances. The heat of the water circulating in the primary circuit is absorbed by the water flowing in the secondary circulation circuit, which evaporates and rotates the turbine for electricity generation. For reactors of the VVER type, the primary and secondary circuits must be hermetic: the water flowing in the primary, in the absence of system defects, can leak neither to the reactor containment building nor to the secondary circuit. The leakage of the contaminated water from the primary circuit to the secondary circuit increases the risk of contamination of the environment with radioactive substances.

the secondary circuit. Such defects are not typical to the newly build nuclear reactors. Despite the identified defect, the operation of Unit 1 of the Belarusian NPP was renewed without taking all the precautionary measures and thorough investigation.



Model of Rosatom's VVER type reactors
rosatomnewsletter.com

Disregarding all the technical defects in the NPP, Rosatom was seeking to get the licence for the commercial operation of Unit 1 as soon as possible. The organisation put pressure on Belarusian experts and sought support of the Belarusian political leadership. Belarusian regulatory institutions doubted that the license for commercial operation of Unit 1 could be issued due to the incidents, defects and failure to meet the requirements. However, due to the pressure from the highest Belarusian political authorities and Rosatom, the licence was granted. It is obvious that the license for commercial operation of Unit 1 was a politically motivated decision and the commercial exploitation of Unit 1 was started without having fixed all the defects and finished all the due tests. The 'historic event' was the result of Rosatom's ambitions, negligent attitude towards nuclear safety requirements and political pressure on Belarusian regulatory institutions.

Likhachev's praise for the highly qualified professionals, who carried out work in the NPP, also raises reasonable doubts. Belarus had been confronted with a lack of qualified subcontractors and personnel since the start of the project, and daily operations at the construction site were characterised by a low working culture. The operation of a nuclear power plant by highly qualified personnel is a key factor in the timely and appropriate response to incidents and their consequences. Belarusian NPP experts, due to the lack of expertise, must rely on the support from Rosatom or other Russian institutions. It reduces the likelihood of a timely and adequate response to incidents, which could lead to a risk of contamination of the environment with radioactive substances.

There is no shortage of various disruptions in the NPP following the start of its commercial operation. On 12 July 2021, Unit 1 disconnected from the power transmission network in an emergency mode. The reactor was relaunched only on 4 October 2021, but was subsequently stopped several times. In October 2021, leakages in the primary circuit were identified once again.

Rosatom and Belarusian authorities constantly conceal information about the actual situation in the NPP. Since the beginning of the project, they have not provided detailed information about the incidents that occurred during

the construction of the NPP and have concealed information on the hasty course of work, the lack of expertise and a careless approach to nuclear safety requirements. However, it did not lead to a risk of polluting the environment with radioactive materials. A nuclear power plant, when operated without due care, may witness incidents with more serious consequences. It is highly likely that concealment of information on the actual situation will limit the possibilities to respond to the incidents in an appropriate manner.

RUSSIA EXPLOITS ENERGY LEVERS TO ADVANCE ITS INTERESTS

In 2021, the manipulation of the Russian gas company Gazprom on the natural gas market became clearly obvious. Russia's main objectives in the field of energy are to start operating the Nord Stream 2 gas pipeline as soon as possible, restore the influence and positions in the market that have been lost in recent years due to the development of the liquefied natural gas (LNG) market, and to maintain Russia's energy infrastructure links with Europe.

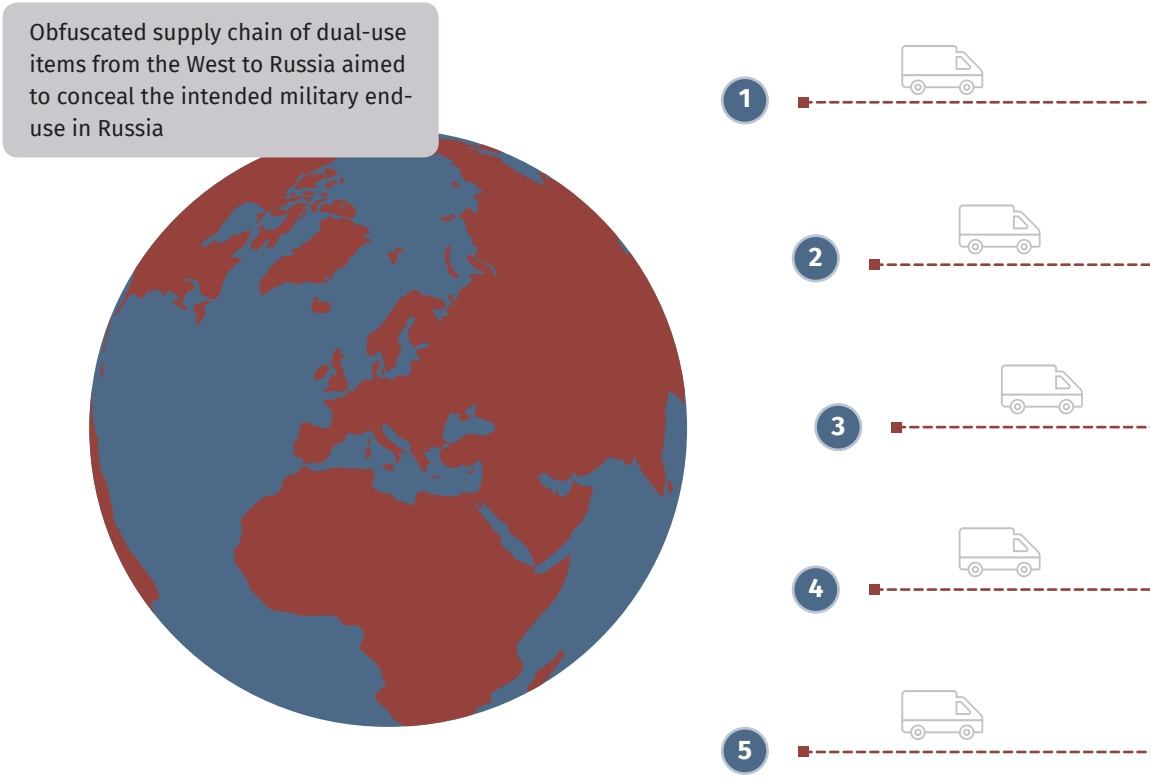
In mid-2021, Gazprom reduced the natural gas supply to the European market and natural gas storage to the minimum allowed within the existing contracts. Russia also sold smaller than usual volumes of natural gas on the spot market. Natural gas prices started to rise rapidly and hit unprecedented highs. Conducive conditions for manipulation in LNG market were created by its short supply. Equinor, Europe's largest LNG plant, was not operating due to a fire in September 2020, while even higher natural gas prices in Asian countries diverted the LNG deliveries to this region.

Representatives of the Kremlin had openly declared that the problem could be solved by launching the Nord Stream 2 pipeline, speeding up the licensing processes and issuing all the necessary permits for its operation. Gazprom indicated that the pipeline would allegedly provide additional quantities of natural gas and would solve the gas crisis in Europe. Gazprom, using already existing infrastructure, had technical capacities to increase natural gas supplies, though it was not done. It is highly likely that the Kremlin sought to accelerate the start of the operation of Nord Stream 2.

In order to achieve its political objectives, Russia does not avoid using its leverage in other energy sectors. Synchronisation of electricity systems with continental European networks is a priority project for the Baltic States to ensure their energy independence. It is highly likely that in the near term Russian authorities will seek for ways to influence decisions on this project in order to maintain infrastructure links with the Baltic States. They are likely to develop new or take advantage the already existing ties with representatives from energy enterprises operating in the Baltic States, to strengthen lobbying activities in the EU institutions or to manipulate early disconnection of the Baltic electricity systems from the BRELL ring.

RUSSIA SEEKS TO ACQUIRE MISSING WESTERN TECHNOLOGIES FOR INTELLIGENCE AND MILITARY PURPOSES VIA INTERMEDIARIES

Due to the economic sanctions imposed in view of Russia's actions in Ukraine, the Russian military industry faces restrictions in acquiring dual-use items needed to fill in its existing technological gaps. In order to circumvent the restrictions and avoid controls, Russia uses the services of intermediary companies established in the West and wholesalers in Russia to conceal the dual-use nature of the goods and the intended end-use. Russia's military industry is likely to remain dependent on Western technologies in the near and medium term, so the need for intermediary services will remain high because of the restrictions applied on Russia.



To circumvent these restrictions, Russia exploits logistics operations in Lithuania, among other transit countries. Logistics companies and other intermediaries, responsible for the implementation of Russian orders, organise the export of goods from or transit via Lithuania. While conducting customs procedures, they often seek to conceal information about the dual-use nature of the exported goods and actual end-users in Russia. Such data must be submitted when applying for a licence to export dual-use goods.

Control authorities decide to grant a licence after a thorough risk assessment and after making sure that dual-use items are not intended to use for military purposes and by military end-users. The end-users of goods declared to the customs are often companies engaged in wholesale trade in Russia. In this way, transit countries become involved in obfuscated commodity delivery chains designed to circumvent international restrictions and to conceal real end-users in Russia due to their links with the military industry.

Production and sales of dual-use items

Manufacturers in the West sell dual-use items and technologies

Sales and logistics intermediaries in the West

Intermediary companies established in the West obtain technologies and re-sell them to other intermediary companies

Export from the West to Russia

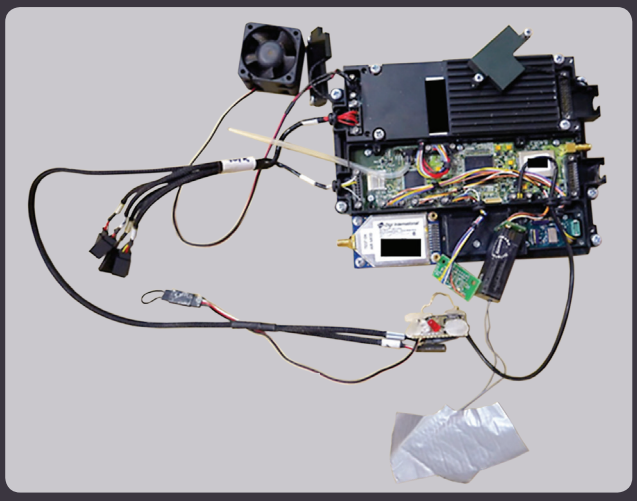
During the procedures of customs export, intermediary companies conceal the purpose of controlled dual-use items and the actual end-user in Russia

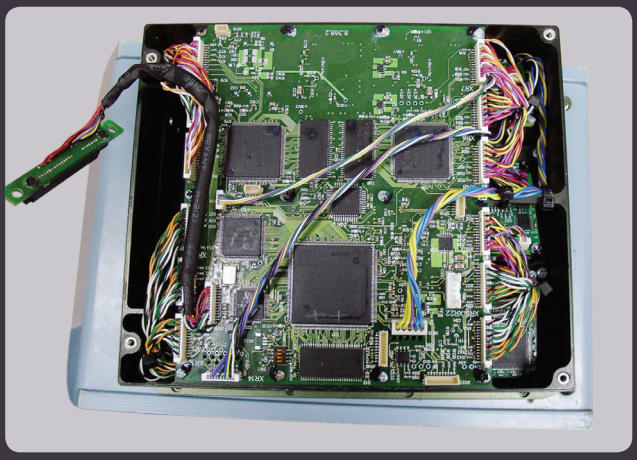
Intermediate users in Russia

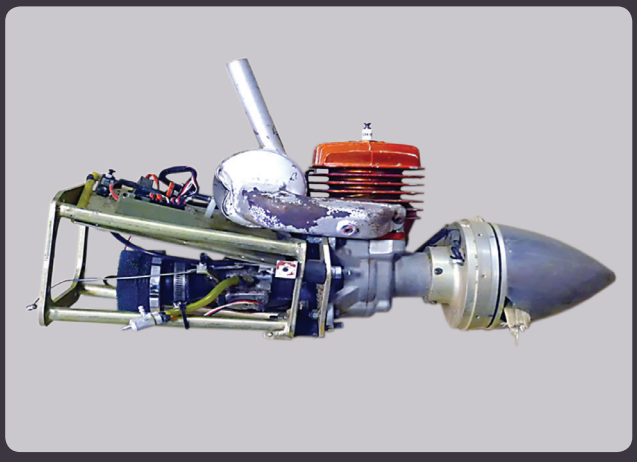
Wholesale companies in Russia sell technologies to science and education institutions implementing military research programmes, or to the representatives of military industry

Final military use in Russia

Final end-users in Russia use these technologies in the development programmes of mass-destruction weapons







Components of Western manufacturers were used in the production of the Russia-related reconnaissance UAV found in the territory of Lithuania.

A recent study by the Conflict Armament Research (CAR) organisation in the United Kingdom confirms the use of intermediaries by Russia for circumvention of restrictions and acquisition of Western technologies. CAR established schemes for the acquisition of components used in the production of an unmanned aerial vehicle (UAV) associated with Russia that was found in Lithuania's territory and the UAVs which carried out reconnaissance operations in eastern Ukraine. In 2012, 2014 and 2015, ultra-precision gyro and accelerometer modules installed in these UAVs were purchased from EU manufacturers by Radiant-Elcom (currently renamed Radiant Group), a distributor of electronic components in Russia. Subsequently, they were sold to other Russian customers engaged in scientific research. Afterwards, Radiant Group also sought to arrange the supply of similar Western production equipment to Russia, but control authorities halted such exports due to the risks of using the equipment in military programmes.

The CAR study also confirmed that Russian contractors in the West are involved in the technology supply chain to Russia. Engines manufactured in one Western country were used in the production of Russian reconnaissance UAVs and were supplied to Russia through an intermediary, a Russian-owned trading company established in another Western country.

NOTES

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

17.02.2022. Circulation: 831 units. Order GL-5

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 2669-2724

© Ministry of National Defence Republic of Lithuania, 2022

© State Security Department of the Republic of Lithuania, 2022