NATIONAL THREAT ASSESSMENT 2021
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. Based on them and considering the long-term trends affecting national security, the document provides the assessment of major challenges that the Lithuanian national security is to face in the near term (2021–2022). The assessments of long-term trends project the perspective up to 10 years.

The assessment is based on the information available before 5 February 2021.

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

<table>
<thead>
<tr>
<th>&lt; 25 %</th>
<th>25–50 %</th>
<th>50–75 %</th>
<th>&gt; 75 %</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNLIKELY</td>
<td>POSSIBLE</td>
<td>LIKELY</td>
<td>HIGHLY LIKELY</td>
</tr>
</tbody>
</table>

Short term: 0–6 months    Near term: 6 months – 2 years    Mid term: 3–5 years    Long term: 6–10 years
Darius JAUNIŠKIS
Director of the State Security Department of the Republic of Lithuania

Colonel Elegijus PAULAVIČIUS
Director of the Defence Intelligence and Security Service under the Ministry of National Defence of Lithuania
Dear readers,

This is the sixth edition of the National Threat Assessment prepared by the State Security Department of the Republic of Lithuania and the Defence Intelligence and Security Service under the Ministry of National Defence of the Republic of Lithuania.

Lithuania is the only country in the region and one of the few in the world whose intelligence services provide a joint public threat assessment. It enables our society, decision makers, officials, security experts and foreign partners to receive an overall picture of the regional and global threats, the relevance and significance of which are acknowledged by the entire Lithuanian intelligence community.

The main mission of Lithuanian intelligence services is to collect information, analyse it and assess threats to our state and society emanating from hostile foreign countries, their armed forces, intelligence and security services, economic influence, disinformation as well as from individuals willing to commit acts of radical extremism or terrorism – all what is encompassed by intelligence services’ scope of activity.

The geographical position of Lithuania itself preconditions that sources of major emerging threats remain the same. However, threat manifestations and conditions are changing dynamically. The COVID-19 pandemic not only poses a threat to our people’s lives and health, but it also gives grounds for cyberespionage, conspiracy theories and disinformation against Lithuania. Russia and other authoritarian countries exploited pandemic containment as a pretext for adapting new public control measures that impose even more severe restrictions on democratic freedoms.
Belarusian authoritarian regime is striving to suppress its nation’s peaceful protests by employing violence and repressions. The Kremlin provides political, financial and military support to authoritarian Minsk. The instances of Russian rapid military deployments and the demonstrative manoeuvres in Belarus are intended to send a message that Belarus belongs to the Russian sphere of influence. It is almost certain that Russia’s policy of denying the sovereign choices of its neighbours will remain one of the most significant security threats in the Baltic Region in the future. Russian and Belarusian strategic military exercise Zapad–2021 due to take place in September 2021 will increase the risk of military incidents and provocations.

In today’s fast changing environment the flow of information can hardly be covered, so only reliable sources shall be referred to when assessing relevant issues to Lithuanian national security. By presenting this Threat Assessment, intelligence services of Lithuania seek to provide information which would allow every member of its society to make objective and fact-based judgements rather than rely on rumours or speculations. Although in many cases we cannot provide detailed information related to threats, as a considerable scope of intelligence information is classified, the assessment reflects the most significant trends of the threats to Lithuania. By informing our society we intend to enhance confidence and trust in the intelligence services, the lack of which would make an intelligence officer’s work impossible.

The State of Lithuania is strong so long as its residents, friends and partners are informed, aware and united. The National Threat Assessment prepared by the VSD and the AOTD is expected to contribute to strengthening of the state and society.
The COVID-19 pandemic is a game changer in the global threat landscape and poses not only medical but also social, economic and geopolitical threats. Authoritarian states abuse the tool of contact tracing to expand mass surveillance of their citizens and foreigners. Russia and China exploit the pandemic to discredit perceived adversaries or, on the contrary, to improve their own international image. The two states use medical support and innovations as a power tool to expand their influence in the international arena. In many countries the spread of radical political ideologies and destructive conspiracy theories is increasing due to the pandemic. To a lesser extent the trend is also observed in Lithuania.

The political crisis in Belarus is the most significant development taking place in the vicinity of Lithuania. It is highly likely that no future Belarusian political leadership will be able to ignore the role of its strengthening civil society. Massive protests that burst out after the rigged presidential election indicate that Alyaksandr Lukashenka and his political regime are no longer capable of genuinely responding to society’s needs and thus, of maintaining its support. The situation in Belarus will be conditioned not only by society’s ability to organize and Lukashenka’s capabilities to sustain the officials’ loyalty but also by Russia’s determination to strengthen its influence in the country.
The use of the Belarusian Armed Forces and power structures in domestic affairs escalates tensions in Lithuania’s neighbourhood. The Belarusian foreign and security policy will likely remain adherent to Russia in the mid term. So far Lukashenka has managed to avoid permanent presence of the Russian Armed Forces’ combat units in Belarus, but it remains a possibility if the Belarusian regime weakens. The unprecedented demonstration of force of the Belarusian Armed Forces with the aim of countering the alleged threat from the West and Lukashenka’s determination to remain in power at all costs pose a risk to Lithuanian security. In the meantime, the State Security Committee of Belarus (KGB) continues to perpetrate aggressive intelligence activities against Lithuanian citizens in the territory of Belarus.

In autumn 2020, Belarus hastily launched the Belarusian Nuclear Power Plant (NPP) without completing due system tests critical to its safe exploitation. The NPP poses a high risk to Lithuania’s national security as Belarusian authorities continue to neglect expert conclusions on safety requirements and to conceal information about the incidents. The industrial exploitation of the NPP starts in 2021. Belarus also aims to circumvent the restrictions and to sell electricity produced in the NPP to the Baltic States.
Isolated, repressive and resentful Russia poses a major threat to Lithuania, as it feels less constrained not only by international law but also by international opinion. Strengthening its power, Russia’s ruling regime imitates democratic processes but crushes its opponents. In terms of international relations, acting aggressively, Russian authorities increase their isolation and conflict possibilities. Russia has not abandoned its strategic objectives in the current and former members of the Commonwealth of Independent States (CIS), but it is struggling to achieve them.

The military power remains the main tool for Russia to maintain and expand its influence abroad. Amid the COVID-19 pandemic, Moscow announced its aims to deescalate military tension between Russia and NATO, but aggressive manoeuvres of the Russian Armed Forces near NATO borders proved the opposite. Russia’s preparedness to exert influence by confrontational – including military – means over its opponents will persist. Russia’s growing military potential will pose a threat to the national security of Lithuania.

Russia’s intelligence activity against Lithuania remains persistent. Due to the COVID-19 pandemic, the extent of Russia’s human intelligence activities against Lithuania has decreased. Despite movement restrictions, Russian services actively conduct intelligence in Lithuanian municipalities bordering the Kaliningrad Region. The rise of remote work and electronic services also increased the cyber espionage threat.
Russia increasingly relies on legal means and advances their extraterritorial application to pursue its historical policy abroad. The Russian Investigative Committee brought criminal charges in absentia against three Lithuanian judges, who had been investigating the 13 January 1991 Soviet aggression case, and put them on the international wanted list. In accordance with the amendment of the Criminal Code of Russia that established criminal liability for destruction or damage to graves and statues of Soviet soldiers abroad, the Investigative Committee has already launched several investigations – including those related with the incident in Lithuania.

The number of cyber-enabled information operations against Lithuania is increasing. Foreign actors concurrently employ disinformation and cyber manipulations against Lithuania and its allies. Such operations aim to weaken transatlantic ties, sow discord in society and undermine public trust in state institutions.

Although terrorism remains a major threat in Europe, the threat level in Lithuania is low. Individual Islamic extremists conduct more attacks against random people and officers in Europe. Terrorism propaganda online was a source of inspiration and motivation to violent attacks for most extremists. The Internet becomes the main indoctrination and coordination tool of right-wing extremists, including in Lithuania.
NEW SECURITY CHALLENGES

THE COVID-19 PANDEMIC ESCALATES NATIONAL AND GLOBAL THREATS

The world has faced dangers to the public health posed by pandemics before, however, the COVID-19 pandemic is not merely a health crisis. It led to restrictions of public life, affected the role of the state and multilateral cooperation. The pandemic accelerated the existing political, economic and social challenges and prompted their further escalation.

Initial reaction by many states towards the global COVID-19 outbreak revealed a common trend of prioritizing national interests over collective actions. Sudden introduction of travel restrictions, competition for medical equipment and other national restrictions imposed to contain the pandemic contributed to the emergence of such a trend.

The COVID-19 pandemic caused and increased threats

- Xenophobia
- Disinformation
- Cyber attacks
- Tracking and surveillance technologies
- Diplomatic pressure
- Economic decline
- Postponed elections
- Isolationism
Authoritarian states have exploited the pandemic to convert the contact tracing – one of the main tools for virus containment – into a vast surveillance system, which enables a centralized collection of personal data and control of movement in public areas, including uninfected individuals and foreign citizens. China has expanded its national surveillance system and introduced a national health code. The code has become an integral part of Chinese authorities’ effort to manage people’s movement in and out of the affected areas, public transport or other places such as restaurants. To receive the code, people are obliged to upload personal information, medical records and travel history to China’s most popular mobile applications. Once the authorities have approved the data, an individual receives green, yellow or red code that allows or prohibits movement in public areas. Mass surveillance by CCTV cameras and drones continues as well.
Russia has also applied a similar system. Moscow residents over 14 years old, willing to visit public areas, had to request a special QR code. To receive such a code, one must link up own personal account on the licence site with the e-Government (a system storing personal data). In addition, Moscow has updated face recognition system on 100,000 CCTV cameras. Although such renewal of CCTV cameras is mostly related to the development of smart cities, it also provides the authorities with a possibility of increasing mass surveillance and maintaining a centralized information control in their disposition.

Authoritarian states also exploit the pandemic to achieve global goals – either to undermine the West or to improve their own national image. Russia has swiftly adapted to the evolving international security situation to spread the pandemic related propaganda and disinformation in the West. In order to sow confusion and disseminate COVID-19 related conspiracy theories, Russian propaganda usually entails unrelated or even contradictory narratives regarding the shortcomings in containing the pandemic internationally. Thus, Russia maintains its traditional strategic interests – to incite conflicts among Western countries and stir domestic disputes, to support Eurosceptic movements and to demonstrate an alleged inefficiency of the EU, NATO and their Member States.

Chinese propaganda and diplomacy towards the EU or its particular Member States have become more prominent during the pandemic in order to counter international criticism about China’s initial poor handling of the coronavirus outbreak and to shape a positive national image. In such narratives, China is usually positioned as the first global economic power to have successfully contained the virus and to have quickly recovered, as a state, which provides support to multilateral cooperation and to the countries more affected by the virus. Chinese authorities not only aim to restore the country’s global reputation, but also strive to strengthen political influence by providing medical equipment as humanitarian aid to the countries facing the pandemic.
CHINA EXPLOITS THE PANDEMIC TO EXPAND ITS INFLUENCE IN LITHUANIA AND OTHER COUNTRIES

During the pandemic, China’s political regime – with the Chinese Communist Party (CCP) ahead of it – engaged in ‘mask diplomacy’ with massive propaganda campaigns being its key feature. Chinese diplomatic missions play an important role in such type of diplomacy, since they supervise the supply of medical equipment and concurrently ensure that people are aware that the aid was provided by China. International Chinese corporations are also actively involved – by donating medical supplies they seek to gain publicity along with competitive edge in the recipient country. China’s authorities engage in propaganda campaign directed towards foreign audience through various influence channels such as diplomatic missions, news agencies, international corporations, diaspora and student organizations, as well as informal ties with politicians, journalists and scholars. Propaganda related narratives depict China as a global leader and promote achievements of the CCP, while at the same time they highlight the lack of solidarity among democratic states.

- In order to improve the image and competitiveness of its international companies, China’s political regime coordinated shipments of medical equipment to Lithuania. China publicly portrayed the shipments as aid from its international companies that have direct interests in Lithuanian telecommunications and energy sectors.

- In order to control pandemic related narratives, China’s political regime strengthened cooperation with Lithuanian media outlets by regularly ordering sponsored articles. The topics varied from China’s achievements in fighting the pandemic, humanitarian aid and benefits of Belt and Road Initiative to criticism towards Lithuanian politicians and activists, who publicly raise concerns about China’s human rights violations as well as the regime’s policies regarding Hong Kong, Tibet and Taiwan.

- China’s authorities attempt to expand their influence in Lithuania through Chinese Embassy and other associated structures such as Xinhua news agency’s local office, China Chamber of Commerce in Lithuania and the Association of Chinese Diaspora.
Beijing and Moscow have been heavily criticized for the lack of pandemic management capabilities; however, both countries have invested significant resources in vaccine development and manufacturing, eventually using the coronavirus vaccine as a new geopolitical instrument of global influence. China’s aim is to have its vaccine used in as many countries as possible, especially in the developing ones. It has been steadily expanding bilateral partnerships with Latin America, Africa and Southeast Asia. Russia considers the vaccine development as an opportunity to improve its international image and partnerships with India, Brazil, Venezuela, Belarus and other countries. Russian authorities have announced that dozens of countries are willing to purchase the Russian vaccine, with Belarus given the priority as it has contributed to the vaccine trials.
PUTIN’S POLITICAL THEATRE STRUGGLES TO IMPRESS AUDIENCE AT HOME AND ABROAD

In the beginning of 2020 Vladimir Putin promised changes in Russian politics. He reshuffled the government and initiated constitutional amendments. Putin personally made a promise that the government would be accountable to the parliament and spoke against abolishing presidential term limits. Moreover, he even suggested that the word ‘consecutive’, which enabled his comeback to the Presidential office in 2012, should be removed from the constitution.

Putin’s promises were hollow. The constitutional amendments and the subsequently adopted constitutional laws strengthened the president’s power to appoint ministers and other state officials. In addition, Putin has secured his term in the office at least until 2036. The Kremlin conducted a true political spectacle to adopt constitutional amendments. The first Soviet female cosmonaut Valentina Tereshkova pretended to put forward an unexpected proposal that the two-term limit should only apply from the next presidential election. Tereshkova, a member of the State Duma, argued that during her meetings with the electorate she had found out that people feared Putin’s exit. Putin himself visited the State Duma a couple of hours later and endorsed the proposal. The Federal Assembly and all Russia’s regional parliaments approved the package of constitutional amendments in four days.

To demonstrate public support for the continuity of Putin’s presidency the ruling regime organized a weeklong ‘All-Russian vote’. According to the Russian law, the popular vote was not even mandatory. The voting procedure lacked legal regulation, which enabled unprecedented manipulations of the democratic process. Polling stations were set up at work places and residential areas, such as the backyards of apartment complexes. The electorate was
motivated with games and souvenirs. The authorities impeded the activity of independent observers, whereas no limits were applied to the official propaganda campaign for constitutional amendments. The Kremlin had already used such new campaigning and voting practices in regional elections. It is highly likely that the regime will further elaborate and use them for gaining desirable results in the upcoming elections to the State Duma in 2021.

A large part of Russians believe in the regime’s propaganda, which presented the constitutional amendments not as an extension of Putin’s rule but as an entrenchment of national values and effort to improve social welfare by indexation of wages and pensions. Others see no alternative to the current ruling regime mainly because the regime effectively eliminates such emerging alternatives by naming any opposing party a ‘foreign agent’, prosecuting political opposition and civil society activists. The discontent with the regime rises slowly, society seeks for alternative sources of information and expresses its dissatisfaction in protests. So far, such protests are regional and mostly driven by local issues. The regime does not consider them as a threat to political stability, not even those in Khabarovsk that lasted over a hundred days. However, such protests revealed a new trend – the involvement of previously completely loyal groups. In several years, the situation in Russia could resemble the current crisis in Belarus. Passive support could suddenly disappear and the ruling regime could expect to retain power only by resorting to violent repressions.

RUSSIA’S RULING REGIME POSTPONES PLANS OF ECONOMIC AND SOCIAL DEVELOPMENT

As a result of the COVID-19 pandemic, Russia’s GDP in 2020 decreased similarly to the global economy. However, the capital outflow and the depreciation of rouble reveal Russia’s deeper economic problems. The international sanctions also limit investment and development of innovative technologies. Russia’s economy has faced serious difficulties since 2014, and the Kremlin tried to boost the country’s development by initiating extensive investment programs. The pandemic further complicated their implementation that was stumbling due to the regime’s bureaucracy and corruption. Putin decided to postpone the implementation of the National Program from 2024 to 2030 and replaced the specific ambitious goals with ambiguous phrases.
The Kremlin turns back to a well-tested survival policy, where the needs of the regime are financed by exporting resources and the citizens cover the costs of macroeconomic stability. This ensures the supposed stability that is increasingly emphasized by the regime’s propaganda. However, economic problems erode public support for the regime and no propaganda can hide its kleptocratic tendencies. During the pandemic, the state aid was mostly provided to large state companies and businessmen related to the regime. Russia plans budget cuts, but those are unlikely to apply to influence operations abroad and to power structures that ensure stability at home.

One of the most vocal critics of the Kremlin’s regime Alexey Navalny was poisoned in Russia on 20 August 2020. Independent laboratories in several countries and the Organisation for the Prohibition of Chemical Weapons (OPCW) identified that Navalny had been poisoned with a nerve agent belonging to the Novichok family of chemicals. It is highly likely that Navalny was poisoned by order or with the approval of the highest echelons in the Kremlin. The Kremlin’s regime immediately launched a coordinated campaign to conceal the fact of the poisoning. It lied about Navalny’s condition, delayed his transfer from the country, did not investigate the case and later ignored publicly revealed facts about the Federal Security Service’s (FSB) activities in the poisoning operation. Similarities to other assassination attempts abroad (Alexander Litvinenko, Sergey Skripal, Emilian Gebrev) increase suspicions that it is the regime’s responsibility.

The assassination attempt on Navalny shows that for the sake of retaining power the ruling regime is determined to resort to ultimate measures. The Kremlin considers Navalny to be one of the most dangerous opposition activists. He and his supporters have been increasingly subjected to traditional repressions (prosecutions, arrests, fines and expropriations of companies’ assets) but continued opposition activities nonetheless. Navalny was poisoned during his trip to Novosibirsk and Tomsk to investigate corruption. In regional elections that took place after the poisoning, the ruling party ‘United Russia’ received fewer votes than in the previous elections, while Navalny’s allies were elected to the local councils.
Russia continues to deny the fact of poisoning and conducts a coordinated disinformation campaign seeking to confuse domestic and international audience. It presents most incredible versions of the events, accusing the West and the Russian opposition of poisoning and provocations against Russia. Russia’s top officials who are personally involved in the propaganda campaign discredit themselves and demonstrate their disregard to law and morality. Even though the Kremlin would like the international opinion to change, it is not willing to change its own actions and so it further reduces possibilities for trust and dialogue in the international arena.

The Kremlin is unlikely to modify its rhetoric and policy in the short term. It has been rebuffing concerns of the international community about authoritarianism and human rights violations as hypocrisy that serves to weaken Russia as well as considering internal criticism of the regime as a venality for a long time. Isolation is the new trend of Russia’s foreign policy. It is based on perception that if the West, the EU and particular countries cannot accept the cooperation on Russia’s terms, the Kremlin itself should redefine relations with them. As a neighbouring country, the isolated and resentful Russia would pose a greater threat to Lithuania. It is likely that Russia’s influence in the neighbouring countries aimed at neutralizing alleged external threats will become the Kremlin’s priority, and Russia’s actions will be less constrained not only by international law but also by international opinion.

**CIVIL SOCIETY REVEALED LIMITS OF LUKASHENKA’S REGIME**

The year 2020 became a milestone in the recent history of Belarus. Despite being labelled as apolitical, Belarusian society mobilized against the rigged presidential election. For the first time since the election of Lukashenka as the president of Belarus in 1994, civil unrest has reached a massive scale – with daily numerous demonstrations not only in Minsk but also in other regions. Protests consolidated Belarusians from different social backgrounds; furthermore, effective use of social media and innovative protest forms showcased ingenuity of the protesters.
As the Central Election Commission of Belarus began the registration of candidates, it became evident that 2020 presidential election would become a turning point in the country’s politics, which had been dominated by Lukashenka for decades. Political newcomers, such as Syarhey Tsikhanouski, Viktar Babaryka and Valery Tsepkala, who were neither members of opposition parties nor had any previous political experience, appeared to be able to pose a challenge to Lukashenka due to their potential to secure the support of the significant portion of Belarusian society.

The falsified election caused public outrage, but lasting inadequate policies of the authoritarian regime were the main reason behind mass civil mobilization and the longevity of the protests. Decade-long economic stagnation created the feeling of insecurity about the future and the sense of financial instability. The regime’s lax attitude to the COVID-19 pandemic made citizens of

---

On 16 August 2020, Belarusians gathered in Minsk for an unprecedented protest against the results of presidential election and the use of violence against peaceful protesters

*Scanpix*
Belarus anxious about personal health and wellbeing of their families. While the rest of the world was introducing strict quarantine measures, Lukashenka downplayed global reaction by naming it a psychosis, recommended vodka and agricultural work as reasonable treatment, whilst ignoring the fact that hospitals in Belarus were filling up with COVID-19 patients.

The COVID-19 pandemic and post-election political crisis revealed the regime’s inability to address critical situations. As loyalty had always prevailed over competence throughout the civil service in Belarus, public officials lacked knowledge and flexibility to manage emerging threats. Although the security apparatus diligently defended the regime, its loyalty rests solely on financial incentives and fear rather than on the dedication to nation’s interests.

The Kremlin’s economic support – mostly in a form of subsidized energy resources – has been pivotal to the Belarusian economy and helped the regime to maintain an informal contract with Belarusian society. Russian subsidies have enabled Lukashenka to stay in power without any necessity to address the country’s ineffective Soviet-style economic model. However, subsequent economic dependency has become Russia’s instrument to seek political influence on Belarus. Meanwhile by orchestrating violence against peaceful demonstrators, Belarusian regime has lost the ability to secure Western financial support, thus remaining with Moscow as the only financial donor.

The Kremlin’s long-term objective is to maintain and enhance Belarus’ dependence with the help of various integrational projects – starting with the Union State. The political crisis in Belarus forces the Kremlin to prioritize the stabilization of the situation in the neighbouring country, while the implementation of the Union State at any cost poses unacceptable risk that Belarusian anti-regime sentiment might turn against the Kremlin itself.

Belarusian society's engagement in political activities stimulated the formation of the national identity and civil society and thus presented an opportunity to reclaim the country usurped by the regime. It is highly likely that no future Belarusian political leadership will be able to ignore the role of the strengthening civil society.
RE-ELECTION OF LUKASHENKA IS INSEPARABLE FROM VIOLENCE AND MANIPULATIONS

The regime sought to control the election process and did not consider changing its usual tactics – the dictator claiming to achieve a landslide victory in the first round with over 80% of votes. The regime authorities arrested or otherwise eliminated Lukashenka’s main opponents from the election campaign. Sviatlana Tsikhanouskaya was allowed to run in order to create an illusion that the regime takes public demands for reform into consideration. Strong electorate support for the allegedly weak candidate Tsikhanouskaya and the exposure of the gross violations during the election were sufficient to provoke disappointment and outcry.

The Embassy of Belarus to Lithuania also attempted to rig the results of the election. Belarusian officers conducted time-consuming inspection of documents and metal detector checks. Only few Belarusian citizens were allowed to enter the Embassy at a time, which eventually limited their right to vote. Despite this, Tsikhanouskaya was officially declared the winner in this polling district. After the election, employees of the Embassy observed activists protesting in its vicinity, monitored the anti-regime sentiment in the Belarusian community and took action to suppress it. The Honorary Consul of Belarus in Klaipėda lost his post after publicly declaring support for the protesters.

The regime’s reaction to the protests was extremely brutal – rubber bullets, water cannons and flash grenades were used against the protesters. With arrests of peaceful protesters reaching thousands, testimonies about horrendous cases of torture or failure to provide medical assistance in the detention facilities began to emerge.

Lukashenka aggressively reacted to Lithuania’s position regarding the political situation in Belarus and the fact that with the arrival of Tsikhanouskaya Lithuania became a host for one of the opposition centres. The regime responded with sanctions against Lithuanian citizens, demanded to reduce Lithuanian diplomatic staff in Belarus, sought to influence business community with threats of economic sanctions and tried to influence public opinion. In addition, Lukashenka’s regime intentionally limited bilateral cooperation in preventing third-country citizens’ migration through the Belarus-Lithuania border. The sharpened rhetoric of the regime towards Lithuania and the West in general implies that similar actions can be expected in 2021.
MOSCOW IS STRUGGLING TO ACHIEVE ITS STRATEGIC OBJECTIVES IN CURRENT AND FORMER CIS COUNTRIES

One of the most important long-term objectives of Russian foreign policy is maintaining Moscow’s influence in the former and current CIS countries and preventing their engagement with the West. The Kremlin considers them as part of its so-called ‘zone of interests’ and strives to have political, economic and military developments in these countries aligned with Russia’s interests. However, even military and economic superiority over the current and former CIS countries cannot provide Russia with the necessary instruments to unilaterally achieve its objectives.

Unable to offer equal partnership to the current and former CIS countries, Russia cannot lead by example – neither its domestic nor foreign policy can prove that partnering with Moscow would ensure security and economic prosperity for these countries. Unwilling to abandon its great-power ambitions but unable to exert direct influence over its perceived ‘zone of interests’, Russia has long been trying to solve this problem by using coercive diplomacy – leveraging both threats and use of force to make Moscow’s opponents concede.

By exerting political pressure on the Republic of Moldova, exploiting its energy and economic dependence and secretly funding key political actors, the Kremlin likely expected to maintain its considerable influence on Chisinau. Nonetheless, the former President Igor Dodon – supported by the Kremlin – lost the presidential election to the pro-European candidate Maia Sandu, which indicates that Moscow cannot get its candidate elected easily anymore, even in a country that Russia highly likely considers to have within its sphere of influence.

Since the collapse of the Soviet Union, Russia has also exploited ‘frozen conflicts’ to interfere in domestic affairs of neighbouring states. However, this instrument has been gradually losing its effectiveness. Moscow’s attempts to impose its terms on Kyiv by forcing it to reintegrate the Donbass with local power structures under Russian control have so far been unsuccessful.
The Kremlin will be unable to leverage its control of the Donbass over the foreign and domestic policy of Ukraine as long as Moscow’s demands remain unacceptable to most Ukrainians.

Russia’s vast military potential, however, still enables the Kremlin to achieve short-term foreign policy gains as Moscow successfully brokered a ceasefire agreement in the Second Karabakh War and deployed troops in the conflict zone. While this may have temporarily prevented Ankara from gaining a more significant foothold in the region, Russia can no longer ignore Turkey’s rising power in the South Caucasus. By committing more forces to the region, Russia will also have to carefully balance interests of the warring sides that will seek to advance their own agenda.

Russian military troops in Nagorno-Karabakh
AP / Scanpix
RUSSIA’S OCCUPIED DONBASS: A HOTBED OF MILITARY INSTABILITY ON THE DOORSTEP OF NATO

Moscow-subordinated 1st (Donetsk) and 2nd (Luhansk) Army Corps that consist of brigades, battalions, companies and smaller units operate in Russian-occupied Ukrainian regions of Donetsk and Luhansk. Some 30,000 to 35,000 troops are in service there. Most of them are local residents mainly motivated by remuneration. These formations correspond to the organizational model of the Russian Armed Forces; they are led and trained by Russia's assigned officers and instructors. The units are supplied with Russian armament, equipment, communication systems and comply with Russian statutes as well as procedures; therefore, they can be effortlessly integrated into Russian military operations or interact with units sent from Russia. Moscow can easily increase military pressure on Kiev by using military formations that are completely dependent and fully controlled by Russia. Some of the troops that participated in armed fights against the Ukrainian Armed Forces or were serving in the Corps are employed by private military companies (such as Wagner) with which they conduct the tasks set by the Kremlin's regime and the supporting oligarchs in other conflicts (Syria, Libya, etc.).

THE CEASEFIRE AGREEMENT IN NAGORNO-KARABAKH ENABLED RUSSIA TO INCREASE MILITARY CONTINGENT IN THE SOUTH CAUCASUS

With Russia's mediation, Armenia and Azerbaijan agreed to a ceasefire in November 2020 after six weeks of fighting. According to this agreement, Russia deployed some 2,000 troops at the zone of conflict. This military contingent consists of specially trained contract military service troops who have modern armament and equipment and who previously participated in military operations.

Russia thereby has increased its military presence in the region and has gained an important leverage over further developments of the conflict. Russian forces control the northern part of Nagorno-Karabakh that belongs to Azerbaijan, strategically important Lachin corridor from Nagorno-Karabakh to Armenia (through Azerbaijan) and the road from Azerbaijan to Nakhichevan province (through the southern part of Armenia). In return for security guarantees for Armenians living in Nagorno-Karabakh Moscow gained more leverages to influence foreign and security policy of Yerevan.
RUSSIA’S AGGRESSIVE POWER DEMONSTRATION CONTRADICTS ITS PROMISES TO DEESCALATE TENSION

In late March 2020, Russian Deputy Minister of Defence Col. Gen. Alexander Fomin pledged Russia’s commitment to serious and pragmatic dialogue with NATO by halting military exercises on NATO’s borders. Moscow later announced that Russian Foreign Minister Sergey Lavrov had officially informed Jens Stoltenberg, Secretary General of NATO, about these intentions, while the General Staff of the Russian Armed Forces reported about plans to withdraw the activities connected to strategic military exercise Kavkaz-2020 from the western border inland. Thus Russia allegedly took first step to ‘deescalate’ military threats during the COVID-19 pandemic and invited the international community to join the effort.

However, Kavkaz-2020 had already been planned to take place in the Southern Military District (SMD) – further away from the western borders with NATO. Therefore, Moscow’s rhetoric regarding the suspension of military activities near NATO’s borders only served as an ostensible act of good will. Moreover, some of the activities connected to Kavkaz-2020 took place in routine training ranges in the SMD, including territories of the occupied Crimean peninsula and the Black Sea, where navies of NATO countries also operate.
Numerous other Russian military exercises planned near NATO’s borders were not suspended. The annual large-scale strategic naval exercise Ocean Shield tested the readiness of more than 30 combat ships and support vessels from the Baltic, Northern and Black Sea Fleets as well as the Caspian Flotilla. The exercise also consisted of amphibious warfare training, including a simulated landing of naval infantry on the Baltic Sea coast in the Kaliningrad Region. A two-sided command post exercise of the Baltic Fleet and the 6th Combined Arms Army took place in the Western Military District in August 2020. During this exercise, participants practiced operating against each other, which had not been usual in the Russian Armed Forces combat training for a long time. In October 2020, Russian troops joined other members of the Collective Security Treaty Organization in Unbreakable Brotherhood-2020 drills in Belarus that included more than 700 servicemen and 100 military vehicles.
Nevertheless, the biggest discrepancy between the Russian rhetoric and actions was demonstrated in its reaction to the political crisis in Belarus. On 21 September 2020, while the protests against President Lukashenka were in full swing, Moscow announced that the number of Russian troops intending to participate in the annual exercise Slavic Brotherhood would triple from 300 to 900. Russian airborne troops were deployed to Brest training range near the Polish border the very next day.

On 23 September 2020 – on the same day when Lukashenka was sworn in as president in a secret inauguration ceremony – six Russian strategic bombers Tu-22M3 flew over Belarus near the Ukrainian, Polish and Lithuanian borders. At the same time, two supersonic strategic bombers Tu-160M conducted ground target attacks in Ruzhany training range near Baranovichi. The likely aim of demonstrative flights and deployment of airborne troops was to show that Belarus belongs to the Russian sphere of interests and Russian military can deploy towards NATO borders quickly, unexpectedly and (as opposed to the Belarusian Armed Forces) become a considerable threat to the regional security.

Russian military activity proved that Moscow’s promises to tone down military power demonstration in the vicinity of NATO were deceptive. The Kremlin’s fraudulent rhetoric is used to persuade NATO countries that Russia is ready to engage in a pragmatic cooperation in certain areas of concern (counterterrorism, economic and energy cooperation and fight against climate change). Moscow hopes that some countries will be more willing to foster bilateral relations with Russia and consequently will encourage a review of the common NATO policy towards Russia.

Russian military activities near Lithuanian and other NATO borders will further intensify in 2021. The strategic exercise Zapad-2021 will take place in Belarus, the Kaliningrad Region and the whole Western Military District in September 2021. In fact, Belarus’ military leadership has called 2021 ‘the year of combat readiness’ due to an intended increase of common Russian-Belarusian exercises and other military events by one third compared to 2020. It is highly likely that Russian troops will also be more active in Belarus, and more military activity in the border area usually increases the risk of unintended incidents.
NEW CHALLENGES REDUCED RUSSIAN MILITARY SPENDING BUT LONG-TERM ASPIRATIONS REMAIN STRONG

Although Russia continues to increase its military might, political and military leadership recently had to come into terms with slower than the anticipated economic growth. Fallen oil prices, Western sanctions and lower domestic consumption led to lower budgetary income for 2020. In addition, support to the economy and population due to the COVID-19 pandemic continues to require additional funding. Finally, Russia has announced that its goal of 70% of new or modernized weaponry and equipment in the armed forces by 2020 has been achieved, so the need for expedited investments will decrease. Due to these reasons, Moscow is bound to limit its military funding under the federal budget chapter ‘National defence’ in the short term.

National defence

The majority of the Russian military spending is allocated under the federal budget chapter ‘National defence’. However, a part of military expenditure is covered by funds from other budget lines which are not included in the official budget for defence spending. For example, some of the funds allocated to education, media, social policy or health care are spent to cover armed forces’ housing system, military schools, media outlets and medical institutions for the military. On top of that, the Russian government is allowed to allocate additional funds up to 10% of all budgetary spending for defence and security sectors, if that is considered essential for national interests.

In 2021, the nominal expenditure for ‘National defence’ will be 4% lower than planned. Instead of 3.232 trillion roubles (€35.7 billion) it will receive 3.113 trillion roubles (€34.4 billion). Despite the decrease, military spending will take up approx. 14.5% of all federal budget expenditures (around 2.7% GDP) while the defence sector will become the third most generously funded area. As usual,
more government spending will be allocated to ‘Social policy’ chapter (27% of all budgetary expenditures) but ‘National economy’ chapter will overcome military spending for the first time (15.5% of all expenditures). In comparison, in 2020 ‘National defence’ chapter received 13.9% of federal spending. This proves that despite dissatisfactory economic situation, the biggest possible financing of armed forces remains a priority. Similar trends are likely to continue in the near term.

Although Russian Ministry of Finance suggested even stricter austerity measures (e.g. to reduce the personnel of the Russian Armed Forces by 10%), the Ministry of Defence has rejected such proposals. According to President Putin, Russia has no plans to drastically decrease defence or security spending and suggestions for cutting down the size of the army are merely deliberations among different government institutions.

Although nominal Russian military budget will be slightly smaller, funding for long-term projects and priorities will continue uninterrupted. New military units will continue to be formed and new weapons will be further developed. The build-up and modernization of the Russian Armed Forces will be visible in the vicinity of Lithuania. Deployment of additional tanks to the neighbouring Kaliningrad Region has been observed for several years already. Newly created motor-rifle division is being developed and the Baltic Fleet is receiving new ships armed with Kalibr missiles.
INCREASED TANK CAPABILITY IN THE KALININGRAD REGION

A tank battalion of the Russian Armed Forces usually has 31 tanks. One unit of such a battalion was located in the Kaliningrad Region until 2018. Thereafter a new tank regiment was established, which is typically comprised of three battalions. One additional tank battalion is planned to be formed as a part of the new motor-rifle division from 2021.

Military units in the Kaliningrad Region are gradually equipped with modernized tanks T-72B3M, which increase both defensive and offensive capabilities. This modification of the T-72 tank, introduced in 2016, has been upgraded with several technical and tactical improvements:

- Approx. 15% more accurate gun;
- Increased capability to find the target in night conditions and from a greater distance;
- Approx. 50% more effective new dynamic tank armour protection decreased tank vulnerability;
- More powerful engine and automatic gear box increased manoeuvrability.
One of the Russian priorities for continuous modernization is the Strategic Rocket Forces, which are equipped with weapons that can carry strategic nuclear warheads and attack targets in other continents. Their capabilities are developed by new additions to the Russian missile arsenal and by constantly upgrading their ability to evade the Western missile defence systems.

The nuclear power status that Russia inherited from the Soviet Union has a big symbolic meaning to Moscow. Therefore, Russia was deeply interested in extending the New START Treaty after 5 February 2021. This agreement gives it parity with the US by balancing their nuclear capabilities. The extension is also beneficial to Russia because it ensures that the current tempo of modernization of Strategic Rocket Forces and nuclear arsenal could be preserved within New START limits and helps avoid costly arms race with a wealthier opponent.

On 9 and 12 December 2020, Russian Strategic Rocket Forces, strategic bombers and nuclear submarines conducted ballistic and cruise missile attacks on targets in Russian training ranges. This was also likely an attempt to demonstrate military power before talks regarding extension of the New START Treaty.

AP / Scanpix
WHY ARE NON-STRATEGIC NUCLEAR WEAPONS SO IMPORTANT TO RUSSIA?

Nuclear weapons are divided into two categories – strategic and tactical (or sub/non-strategic). Strategic nuclear weapons (missiles with nuclear warheads) could be used to destroy cities, military bases and other important infrastructure on enemy territory (more than 5,000 km away). Tactical nuclear weapons, on the other hand, can be used at short or medium range (less than 5,000 km) as missiles or nuclear mines and are intended for use on a battlefield, in some cases – even on one’s own territory.

Tactical nuclear weapons hold a special place in Russia’s military planning, since they fill the gap between strategic nuclear capabilities and conventional weaponry (e.g. tanks, artillery systems, war planes and war ships), which is still unable to reach Western quality standards. In addition, tactical nuclear weapons are a useful deception tool since it is impossible for the opponent to tell apart weapons of the same type that are armed with nuclear or conventional warheads.

Russian tactical nuclear weapon arsenal is not restricted by any international treaties. Such constraints are unacceptable to Moscow and, therefore, it is highly unlikely that Russia will ever agree to accept other arms control agreements that put restrictions on tactical weapons.
RUSSIA PAYS A HEAVY PRICE FOR RECKLESS ARMS PROLIFERATION

Although the majority of Russian weapons provisions are legal, Moscow sometimes embroils in scandals connected to arms supplies to countries under international sanctions or non-state actors. The most widely reported incident was the shot down of Malaysian Airlines flight MH17 over Eastern Ukraine in July 2014, which killed 283 passengers and 15 crew members. The airplane was shot with a missile from an anti-aircraft system Buk that belongs to the 53rd Anti-aircraft defence missile brigade (Kursk, Russian Federation). The missile was launched near Snizhne, from an area that was at the time held by pro-Kremlin forces.

Russian military arms provision continues to destabilize the Mediterranean region. In July, Russia was accused of breaking the UN embargo that forbids arms sales to Khalifa Haftar’s forces in Libya. According to information published by the US Department of Defence, anti-aircraft defence systems, including the short range system Pantsyr, are controlled by Russia or its affiliates in East Libya. Armed Haftar’s militia, the Libyan National Army (LNA), have also claimed that they modernized at least two S-200 anti-aircraft systems. It is probable that Russian specialists provided some expertise to them. Libya received the same type of systems from the Soviet Union in 1980s.

In fact, Russia is known to provide conflicts, such as in Ukraine or Syria, with weapons that already were in these countries in order to obscure the new deployment. It is probable that Russia may also use this scheme in Libya to provide LNA with S-200 systems that were supplied to the Libyan government in the past. This would highlight not only Russian attempts to break the arms embargo but also an irresponsible arms supply policy that threatens the safety of military and civilian aviation in the region.
THE BELARUSIAN ARMED FORCES EXPLOITED IN TACKLING THE POLITICAL CRISIS

In 2020, the Belarusian Armed Forces and the country’s defence policy became hostages of Lukashenka’s efforts to remain president at any price. Seeking to preserve his image of the defender of state sovereignty, Lukashenka made an attempt to convince Belarusians of an external enemy threat. During the election campaign, Lukashenka portrayed Russia as an adversary and accused it of sending mercenaries who allegedly were to disturb the presidential election. Shortly after the election, the West was labelled to be the biggest threat again and it was blamed for the massive protests that sparked off right after the election.

With the aim of proving that the alleged Western threat is real, Lukashenka falsely claimed that NATO threatened Belarus by deploying military units on its border, that Poland sought to occupy a part of Belarus, and Lithuania with several other Western countries was trying to interfere in the internal affairs of Belarus. In addition, Lukashenka publicly announced an order to reinforce the state border security, deploy more military units towards the West, and conduct a number of demonstrative military exercises. Sub-units equipped with ballistic missiles Tochka and long range multiple-launch rocket systems Polonez were deployed near the Lithuanian border.
Most of the Belarusian Armed Forces’ units are deployed in Western direction. 

Belarus nuclear Power Plant
Belarus Nuclear Power Plant
Russian Navy Communications Centre
Russian Ballistic Missile Early Warning Radar Station
Belarusian Armed Forces’ units:
- Mechanized brigade
- Artillery brigade
- Missile brigade
- Special Operations Forces’ unit
- Multiple Launch Rocket Artillery brigade
- Air Defence unit

Location of units:
- Vilnius
- Vileika
- Polatsk
- Vitsyebsk
- Lida
- Grodno
- Brest
- Pinsk
- Babruysk
- Minsk
- Asipovichy
- Baranovichy
- Barysaw
NO CHANGE IN BELARUS’ DEFENCE POLICY AND ITS DEPENDENCE ON RUSSIA

As Lukashenka considers Russia a guarantor of keeping him in power and defending Belarus from military threats, Belarus’ defence policy is strongly dependent on Russia. Over the recent years, the interoperability of the armed forces has been maintained in formats of joint Russian and Belarusian Regional Military Grouping and United Regional Air Defence System. Accordingly, joint exercises to keep the ability to operate together at tactical and operational levels are organized. Belarusian forces train in Russian training areas and officers attend Russian military schools as well as the General Staff Academy. Russian and Belarusian military ties will likely remain strong in the medium to long term.

Notwithstanding close military cooperation, permanent deployment of Russian combat units in Belarus is not in Lukashenka’s interest as this would potentially become an additional Kremlin’s influence lever against the Belarusian regime. So far, Lukashenka has managed to avoid it. However, since the regime has got weaker and its dependence on Russia has grown as a result

Nevertheless, all this ostentatious Lukashenka’s activity did not receive much attention in Belarusian society. Although in the beginning Moscow also did not support Minsk’s narrative of the Western threat, in late August 2020, Russian politicians and diplomats started to accuse Western countries of interfering into Belarusian internal affairs and seeking to destabilize the country. Eventually, Russia sent extra troops to the exercise Slavic Brotherhood in Belarus and by military manoeuvres near NATO borders demonstrably showed that Belarus belongs to Moscow’s zone of influence.

Although the intensity of Belarusian military exercises was high and adversarial rhetoric harsh, the regime’s activity has not made a significant impact on Lithuania’s and regional security. However, the continuation of such rhetoric and the unstable regime’s preparedness to take drastic actions in order to preserve power increase tension in the Lithuanian neighbourhood.
of domestic political crisis, it will be increasingly difficult to resist Moscow’s pressure. There are currently two Russian military objects in Belarus: the early warning radar station Volga (Baranovichi) and the Navy communications centre Antey (Vileyka). The agreement on deployment of these objects is to terminate in 2021, but the contract is highly likely to be extended.

Russia remains the main supplier of military armament and equipment to Belarus and the key military partner in the development and modernization of the Belarusian Armed Forces. The implementation of the supply contract on the fourth generation Su-30SM multirole fighters has been underway, and the first aircraft received in 2019 started their combat duty in summer 2020. In 2020, new contracts on procurement of armoured vehicles BTR-82A for two battalions and four Mi-35M multirole helicopters were signed with Russia. Moreover, procurement of modern air defence armament from Russia has been planned for 2021–2025.
Russia is also partially dependent on Belarus. So far, Russia has failed to completely eliminate its dependence on Belarusian-made component parts of military equipment. For example, Minsk Wheel Tractor Plant has been supplying Russia with chassis used for different arms systems: mobile operational-tactical missile systems Iskander-M, multiple launch rocket systems, long range air defence systems, coastal defence missile complexes and strategic mobile missile complexes.

Belarusian air defence is a part of the Russian-Belarusian Regional Air Defence System that protects air space from Kaliningrad to Saint Petersburg.
RUSSIA’S INTELLIGENCE ACTIVITY IN BORDER REGIONS OF LITHUANIA REMAINS INTENSE

The COVID-19 pandemic and government-imposed lockdown decreased the extent of human intelligence perpetrated by Russian intelligence services against Lithuania and shifted their efforts to cyber espionage. Nevertheless, Russian intelligence operations pose a major threat to Lithuania’s national security. After the COVID-19 pandemic is contained and usual traffic across the border is restored, the activities of Russian intelligence services – especially the human intelligence – are highly likely to return to their previous high levels.

Russian intelligence is especially active in Lithuanian municipalities bordering the Kaliningrad Region. The FSB and the Main Directorate of the General Staff of the Russian Federation Armed Forces (GRU) collect intelligence about Lithuanian citizens regularly crossing the border to Russia and seek to recruit
them. Russian intelligence services exploit the border crossing procedures in order to debrief Lithuanian citizens. Russian intelligence officers inquire about their biographies, work experience, service in the Soviet institutions, family members, ties with foreign countries and attitude towards Russia. Russian intelligence officers also interrogate Lithuanian citizens about NATO exercises in Lithuania and military activities in proximity to Russia’s border.

Russian intelligence services target Lithuanian citizens regularly travelling to Russia even if they do not have access to classified information or intelligence collection possibilities. Russian intelligence services usually task the recruited individuals to provide open-source and visually accessible information about

Passport control at Chernyshevskoye border crossing point, Kaliningrad Region. FSB officers often approach foreign citizens during border crossing procedures

*TASS / Scanpix*
Alongside traditional intelligence collection, one of the priorities of Russian intelligence services is to influence political and social processes in Lithuanian regions bordering Russia. Russian intelligence services consider Lithuanian citizens regularly visiting the Kaliningrad Region to be more vulnerable to recruitment as their personal, business and other interests depend on collaboration with Russian officials and Russian intelligence services’ permit to visit Russia.

During the border crossing procedures, FSB inspects the content of the targeted individuals’ mobile devices – checks their contacts, messages and photos. In some cases, during staged examinations and artificially prolonged interrogations, FSB officers install malicious software on mobile devices of the targeted individuals. The malware allows remote interception of calls and correspondence of the device owner and provides access to the camera and microphone of the device.

Alongside traditional intelligence collection, one of the priorities of Russian intelligence services is to influence political and social processes in Lithuanian regions bordering Russia. To accomplish this task Russian intelligence services exploit traditional and online media to disseminate views and publish comments on developments in Lithuania in terms favourable to the Kremlin.
KGB ACTS AGGRESSIVELY AGAINST LITHUANIAN CITIZENS IN THE TERRITORY OF BELARUS

Lithuania is one of the intelligence priorities for the Belarusian KGB. In Lithuania, KGB officers are deprived of permissive conditions to work under diplomatic cover, thus KGB operatives are most active when targeting and harassing Lithuanian citizens on the Belarusian soil. Officers from the Lithuanian police, the Dignitary Protection Service, the State Border Guard Service, judges, politicians, state and municipal officials, and employees of state-owned enterprises as well as journalists who regularly travel to Belarus are of interest to the KGB. Information collection on these targets is initiated as soon as they submit their visa requests.

In 2020, due to the pandemic related travel restrictions, the KGB had limited capabilities to conduct human intelligence across the border. Usually, in order to recruit Lithuanian citizens, the KGB engages in blackmail, exploits personal vulnerabilities, staged or genuine incidents, administrative violations or attempts to lure into ‘honey trap’, i.e. it introduces its target to an individual cooperating with the KGB so that to lure the target into a compromising relationship and then use it for blackmail. In the short term, the KGB is likely to resort to aggressive and intimidating methods against Lithuanian citizens as a reprise for Lithuania’s alleged role in inciting protests in Belarus.

Of note, despite Lukashenka’s assertive rhetoric towards Russia prior to the presidential election, Belarus remains a significant platform for Russia to conduct intelligence against Lithuania. During the political crisis in Belarus, the cooperation between Russian and Belarusian services even intensified, with heads of Russian intelligence and security services visiting Minsk and providing their support.
ATTEMPT OF BELARUSIAN KGB TO RECRUIT A LITHUANIAN CITIZEN

Tomas (34) is married and has children. He is a database administrator in a state institution. Tomas occasionally travelled to Belarus for leisure with his family or on his own. He used to request Belarusian visas in travel agencies or at the Consulate of Belarus in Vilnius. The Belarusian border guards at Medininkai-Kamenyi Log border-crossing point performed several X-ray checks of Tomas’ car and inquired about drug use. Tomas did not attach any significance to such border checks. Later on, Tomas travelled to Belarus with his friends to celebrate a friend’s birthday. At the bar in Grodno he met a lovely Belarusian girl Yelena, who treated him with exceptional attention all the evening. Under the influence of alcohol, Tomas accepted her proposal to go to her place.

The morning after a Belarusian police officer stopped Tomas on his way back to hotel and demanded to provide his ID and mentioned that he was investigating a theft case. Shortly after, a man in civil clothes approached them and insisted on getting into a car parked nearby, where there was another person inside. The men introduced themselves as Alexander and Grigory and started to interrogate Tomas about his job, family and the purpose of visiting Belarus. The men explained that a female Belarusian citizen had been robbed the night before. They informed Tomas that he was the suspect of committing the crime and would be detained. When Tomas asked to call the Embassy of Lithuania in Belarus, Alexander showed him compromising photos taken the night before at Yelena’s apartment and threatened to pass them to Tomas’ wife. Grigory suggested ways to avoid legal prosecution. In return, Tomas was asked to tell about his work, to characterize his colleagues and pass a copy of the database of Lithuanian residents. Tomas was told he would be contacted on a mobile application during his next visit to Belarus. Alexander assured Tomas that it would do no harm to Lithuania and he would even get a possibility for earning some extra money.

Tomas told a friend about what had happened to him and explained that he was not willing to work for the people who had approached him. His friend had already heard of similar recruitment attempts and suggested contacting Lithuanian intelligence immediately. Back in Lithuania, Tomas contacted Lithuanian intelligence, reported about the incident in Belarus and received necessary assistance.

VSD Trust Line 8 700 70007 and e-mail pranesk@vsd.lt

*The name and other personal details identifying the Lithuanian citizen were altered.*
CYBER ESPIONAGE THREAT INCREASED DURING THE COVID-19 PANDEMIC

In Lithuania, as well as globally, increased amount of remote work creates new cyber vulnerabilities, whereas hostile intelligence and security services seek for new ways to increase the effectiveness of their malicious activity.

Cyber espionage groups coordinated by Russian intelligence services pose a major threat to Lithuanian institutions. It is likely that cyber capabilities of Russia and other hostile countries became the main tool for information gathering due to the changes caused by the pandemic. Restrictions on travel and meetings highly likely impede the services’ attempts to gather intelligence using traditional methods and interpersonal contacts. Nevertheless, the efforts to manage the pandemic do not prevent cyber espionage operations.
The adaptation of organizations and individuals to the changes created a favourable environment for new cyber vulnerabilities to emerge. In Lithuania and in other countries, aiming to decrease mobility and the number of contacts among people, the part of employees who remotely connect to their workstations increased, with virtual conferences replacing face-to-face communication. Information technology (IT) administrators strived to adapt to the changes by creating new access, communication channels and tools as fast as possible and therefore, not always prioritizing security. It is likely that new vulnerabilities appeared not only as a result of haste or possible inexperience of system administrators, but also because they were detected in the software used for remote work, that previously being less popular had received less attention from hackers.

While in 2020 a significant increase in the general amount of malicious activity in cyber space was not observed, the targeting visibly shifted. Criminal hackers more readily used ransomware meant to encrypt the data and allow criminals to demand ransom for decryption against hospitals and other healthcare institutions. It is highly likely that hackers are motivated by belief that in order to regain access to data and systems critically important for patients’ welfare these institutions would be more willing to risk paying the ransom. It is possible that part of these attacks were organized by adversarial countries’ cyber groups in order to destabilize the situation in the targeted countries. Apart
from their usual targets, these cyber capabilities also pursued attacks against organizations that have information on measures applied by other countries to manage the pandemic, research on COVID-19 and vaccines for the virus.

The pandemic was also used by hostile intelligence and security services to compel targeted persons to open compromised e-mail attachments or malicious hyperlinks. The subject of pandemic inspires not only curiosity but also fear, anxiety and other strong emotions that also reduce vigilance and awareness of possible cyber threats. The COVID-19 pandemic was also used as a narrative in periodically occurring cyber-enabled information operations in Lithuania.

It is unlikely that hackers’ motivation to pursue malicious activity will decrease in the short term, but growing attention to cyber security issues among both IT administrators and remote work enabling software developers will benefit the fight against heightened cyber threats. It is likely that prevention of newly arisen threats will remain relevant in the long term, since the use of information technologies will continue to grow after the pandemic as well.
EXEMPLARY OF MALICIOUS ACTIVITY DURING THE PANDEMIC IN 2020

- Google warned about criminal hackers and state cyber capabilities abusing COVID-19 topic in their attacks.

- Klaipėda Seamen’s Hospital data of accounting data management and drug verification systems were encrypted during a cyber attack.

- UK, Canada and US announced that APT29 – cyber espionage group highly likely coordinated by Russian intelligence and security service – executed espionage operations against organizations involved in COVID-19 vaccine creation.

- US Department of Justice indicted two Chinese nationals associated with Chinese Ministry of State Security for the computer intrusion campaign targeting businesses involved in COVID-19 research. It was determined that these hackers pursued malicious activity against Lithuanian gaming industry organization in 2017.

- Microsoft announced that GRU-associated cyber espionage group APT28 tried to get the user credentials to the Office 365 software that became more popular during pandemic.

- The first death directly influenced by malicious cyber activity was recorded. It is assessed that a German patient did not survive because of a longer transfer caused by a closer hospital undergoing a ransomware attack.

- All US sites of Universal Health Services, one of the biggest healthcare providers, became victims of a ransomware attack.

- Lithuanian National Public Health Centre was targeted in a cyber attack.
PROTECTION OF CONSTITUTIONAL ORDER

THE KREMLIN’S INFLUENCE OVER THE LITHUANIAN POLITICAL SYSTEM DID NOT INCREASE AFTER THE PARLIAMENTARY ELECTIONS

There were no malign attempts by foreign entities to affect the conduct or the outcome of the 2020 parliamentary elections in Lithuania. Ahead of the elections, without success, some lone pro-Kremlin activists intended to establish...
a new political party, take over an existing one or to collect signatures for running as independent candidates. None of them entered the parliament due to the lack of organizational skills and marginal electoral base. However, Russia highly likely will maintain its interest in gaining political influence by other means, for instance, engaging in international cooperation projects promoted by its lobbyists and political technologists.

**ATTEMPT OF SUPPORTERS OF RADICAL POLITICAL IDEOLOGIES AND DESTRUCTIVE CONSPIRACY THEORIES TO EXPLOIT THE COVID-19 PANDEMIC**

The state of the COVID-19 pandemic is conducive to dissemination of radical political ideologies and destructive conspiracy theories in many countries. In some of them, political radicals organize protests that turn into public unrest and violent incidents. Both the left-wing and right-wing extremists join the protests as they consider such actions as an opportunity to disseminate their ideological views, destabilize the situation and to undermine public trust in the political system.

To some extent, similar trends are also observed in Lithuania. The activity of political radicals correlates with the introduction of the pandemic related restrictions to public and private life. In 2020, several dozens of attempts to organize protests against such restrictions were identified in Lithuania. Some individuals actively engaged against the government-imposed lockdown rules in Lithuania are susceptible to Russia’s disinformation regarding the COVID-19 pandemic, and they contribute to dissemination of pro-Kremlin propaganda themselves. Although protests got neither much attendance nor provoked public unrest or violence, some of the activists demonstrated their organizational skills and ability to conspire.
Overall, rejection of scientific inventions and technological progress based on radical ideological views (known as technophobia) has become a significant idea of political radicals and supporters of destructive conspiracy theories since the outset of the COVID-19 pandemic. Technophobes mostly target health care system and telecommunications infrastructure. Some countries count dozens of acts of vandalism against cell towers and mobile antennas. In 2020, there were no violent incidents of such type in Lithuania, but there were some incitements on social media to commit similar attacks, and attempts to conduct them are likely, as the 5G mobile network is expanding.

The majority of COVID-19 related conspiracy theories are destructive, however, the anti-vaccine theories pose a major threat to the successful containment of the pandemic. In some cases, they are outright baseless and misleading –

Protest against vaccines, 5G and connecting humans to artificial intelligence

*ZUMA Press, Inc. / Scanpix*
for instance, claiming that a tracking microchip is injected with the vaccine for surveillance purposes – but some theories claim to depend on scientific facts, as they explain side effects of the vaccine without actually providing or distorting the available scientific evidence. This diversity of anti-vaccine conspiracy theories tailored to multiple audiences increases the likelihood that scepticism towards vaccination will prevail among segments of society.
INFORMATION SECURITY

THE KREMLIN INCREASINGLY RELIES ON LEGAL MEANS TO PURSUE ITS HISTORICAL POLICY ABROAD

In recent years, Russia has pursued a historical policy which increasingly relied on weaponizing legal norms and advancing their extraterritorial application. For instance, in April 2020, Russian authorities amended the Russian Criminal Code foreseeing criminal liability for destruction or damage to graves or statues of Soviet soldiers. The law applies extraterritorially, with the Investigative Committee in charge of upholding it. In autumn 2020, the Investigative Committee established a special unit, which, among its other duties, is responsible for combating the alleged falsification of history.

The Investigative Committee has already opened several cases on foreign subjects, for instance, regarding the removal of the statue of Ivan Konev, a Soviet army marshal, in Prague, or publication of a book in Latvia that contradicted the Kremlin’s narrative. In 2020, regardless of the ongoing pre-trial investigation by Lithuanian authorities, the Russian Investigative Committee opened a case in accordance with the Russian legislation on the incident in Žiežmariai, a small town in central Lithuania, where a statue dedicated to Soviet soldiers was smeared with paint and graffiti.

Of note, even before the amendments came into effect, there were cases when Russian representatives threatened Lithuanian municipal officials with criminal prosecution in Russia unless they observe Russian terms in renovating and preserving sites of the Soviet military heritage. The number of similar demands is likely to increase in the near-term, as the Kremlin will likely rely on legal persecution to attain its goals in the domain of historical policy as well as other areas.
In another prime example of legal warfare, in 2020, the Russian Investigative Committee brought criminal charges *in absentia* against three Lithuanian judges, who had been investigating the 13 January 1991 case, and put them on the international wanted list. For several years Russia had been collecting personal data of the judges, including by means of espionage. Denial of the Soviet aggression against Lithuania in January 1991 is a part of the Kremlin’s historical narrative.
In addition, Russia continues to discredit the armed anti-Soviet resistance in Eastern Europe. In September 2020, Putin signed a decree foreseeing disbursement of ₽75,000 (approximately €850) to the citizens of the Russian Federation who permanently reside in the Baltic States or Russia and who have participated in the military operations against the anti-Soviet resistance in Lithuania, Latvia, Estonia, Ukraine and Belarus. The signing of the decree was followed by a propaganda campaign highlighting a shift in the Russian stance as it now considers members of the anti-Soviet resistance equal to the Nazis. The smear campaigns against the armed anti-Soviet resistance in Eastern Europe will highly likely remain among the key features of Russia’s historical policy. Resistance movements deconstruct one of the key myths espoused by Russian propagandists that the occupied countries joined the Soviet Union voluntarily.

PRIGOZHIN’S IMPERSONATOR EXPLOITED IN A FAILED INFORMATION OPERATION IN LITHUANIA

Over the past decade entities such as ‘troll factories’ and private military companies related to Yevgeniy Prigozhin, a Russian oligarch close to the Kremlin, have operated worldwide as proxies advancing Russia’s influence. In 2019, the US imposed sanctions on Prigozhin, his companies and assets due to interference in the 2016 US elections. In 2020, the EU put restrictive measures against Prigozhin for violating the UN arms embargo on Libya.

In 2020, Prigozhin’s impersonator was exploited in an information campaign perpetrated against Lithuania. In early 2020, Hawker 800, an aircraft owned by Prigozhin, landed at Vilnius Airport for maintenance but subsequently had to leave without servicing due to the imposed sanctions. At the same time, a person resembling Prigozhin and holding a Russian passport issued in the name of ‘Yevgeniy Prigozhin’ with the same birth date on it as Prigozhin’s – but not real Prigozhin – arrived in Lithuania taking a commercial flight. From the airport the person went straight to the Ministry of Transport and Communications, took a picture in front of the building and went back to the airport for a return flight to Russia. Overall, he spent five and a half hours in Lithuania.
Two weeks later, Prigozhin’s impersonator took a regular flight to Lithuania for a second time. This time his itinerary included taking pictures of the Lithuanian Parliament (Seimas), the National Museum and the Palace of the Grand Dukes of Lithuania. He did not take his return flight scheduled for the same day, instead, he left for Belarus by train on the next day.

In the meantime, the Russian tabloid news website sobesednik.ru covered this story and claimed that Prigozhin had allegedly arrived in Lithuania on his Hawker 800 for a meeting to discuss IT projects with a high-ranking official of the Ministry of Transport and Communications. A subsequent article on sobesednik.ru claimed that Prigozhin had once again come to Lithuania and visited Lithuanian parliament despite being on the sanction list. To add credence to the story, the articles included photos taken by Prigozhin’s impersonator.

Other Russian media outlets picked up the story and added even more fictional details, for instance, claiming that Prigozhin had met not only state officials but business executives as well. One item even asserted that the assistant to the Chairman of the Parliamentary Committee on National Security and Defence had expressed his discontent that there were no restrictions for Prigozhin to visit Lithuanian institutions.

Setting the record straight, Prigozhin’s impersonator did not actually meet any of the state officials or businessmen mentioned in the fake news published on Russian media. The intent of such information campaign was likely to undermine trust in Lithuania’s international commitments and probe for loopholes in the Schengen border control. Despite the resources allocated by the perpetrators, neither in Lithuania nor internationally did the story receive any significant traction.
Prigozhin’s aircraft landed at Vilnius Airport
27 Jan 2020

Prigozhin’s aircraft left Vilnius Airport
14 Feb 2020

Prigozhin’s impersonator returned to Lithuania
26 Feb 2020

Prigozhin’s impersonator left Lithuania
27 Feb 2020

13 Feb 2020
Prigozhin’s impersonator arrived in Vilnius and left on the same day

16 Feb 2020
First publication on Russian news portals

27 Feb 2020
Second publication on Russian news portals

Pictures of Prigozhin’s alleged visit in Vilnius posted in the website sobesednik.ru

Prigozhin’s impersonator (on the left) and Yevgeniy Prigozhin (on the right)

Reuters / Scanpix
LITHUANIA WITNESSED A SIGNIFICANT INCREASE IN NUMBER OF CYBER-ENABLED INFORMATION OPERATIONS

In 2020, the population of Lithuania was confronted with a heavy stream of hostile information, which varied from occasional fake news to long-established anti-Lithuanian narratives. Perpetrators of cyber-enabled information operations aim to disseminate disinformation by cyber means (hacking into news websites or sending spoofed emails by pretending to be an officer, institution or citizen). All of them had an aim to discredit Lithuania’s and Allies’ reputation and inflate the population’s distrust in government and Armed Forces. In 2020, Lithuania experienced nine cyber-enabled information operations, i.e. a higher number than the average annual. A substantial quantitative increase indicates that perpetrators still regard cyber-enabled information operations as an attractive way to shape discussions on various issues in Lithuanian society.

Malign actors constantly put new tactics to the test, but their strategy and main goals remain the same. Cyber-enabled information operations seek to weaken the transatlantic bond, atomize society and weaken its trust in democratic governance. In 2020, operations covered wider geography, in many cases happening simultaneously in Lithuania and Poland. Perpetrators were quick to exploit global and regional issues in their fake stories (COVID-19 pandemic, Defender-2020 military exercise and unrest in Belarus). As usual, spoofed emails from an alleged official or institution followed almost every operation. However, new tactics were observed in November, when a false story was disseminated by mimicking the official portal of Lithuanian Criminal Police Bureau. Often disinformation was spread by burner accounts on social media or in blogs with liberal editorial policy. This approach likely helped to ensure anonymity, get audience’s attention, speed up sharing and partly delay the debunking process.

The effect of cyber-enabled information operations on the perceptions of the general public remains limited, although the propagated ideas resonate with single individuals and fringe groups. Malign actors will highly likely pursue their search for more convincing and impactful means against the target audience in the short term. Globally, artificial intelligence is already used to write...
stories and generate convincing pictures of non-existing persons’ faces. It is possible that these advancements will be applied in hostile information operations against Lithuania in the near term. In 2021, new informational provocations might occur around the biggest regional military exercise conducted by NATO or Russia. It is highly likely that the number of cyber-enabled information operations in the Baltic region will remain high in the foreseeable future.

Mr. Paweł Tadeusz Purski, Third Secretary of the Polish Embassy in Lithuania, was detained upon entering Lithuania

Officials of the State Border Guard Service under the Ministry of the Interior of the Republic of Lithuania, found a lot of money, drugs and weapons at the detainee during a special operation.

Fakes about Lithuania and Poland in 2020
BELARUS HASTILY LAUNCHED ITS NUCLEAR POWER PLANT

In August 2020, following several delays, Belarus made a political decision to initiate the launch of the Belarusian nuclear power plant (Belarus NPP) without completing due system tests critical to its safe exploitation. Despite these circumstances, Belarusian authorities exerted pressure on Gosatomnadzor, the Department of Nuclear and Radiation Safety of the Ministry for Emergency Situations of the Republic of Belarus, to issue a licence for the physical launch of the Belarus NPP. Gosatomnadzor succumbed to political pressure and agreed to issue separate licences for the physical launch and the power start-up of Unit 1 of the Belarus NPP. Subsequently, the power start-up was also initiated without due testing of some systems critical to control of Unit 1, its exploitation and incident management.

In November 2020 alone, there were four unplanned stoppages of the Belarus NPP. Gosatomnadzor made an official comment on the first incident two days later only after the information had already leaked out to the media. Moreover, Gosatomnadzor provided only partial explanation concealing information on other dysfunctions that had taken place at the Belarus NPP. Given the prevailing culture of secrecy, Belarusian authorities are unlikely to give reliable and timely information in case of emergency.
Commissioning of the Belarus NPP and the first malfunctions

- **7 Aug 2020**: Loading of nuclear fuel into Unit 1 was started.
- **Sep 2020**: Nuclear chain reaction was activated.
- **3 Nov 2020**: Electricity produced at the Belarus NPP reached the power grid.
- **8 Nov 2020**: The Belarus NPP was disconnected from the network after explosion of four voltage transformers.

Physical launch of the NPP is a phase when nuclear fuel is being placed into the nuclear reactor core, a critical state of the reactor is caused and required physical experiments are conducted.

On 7 November 2020 Lukashenka inaugurated the Belarus NPP

*AP / Scanpix*
There are no significant improvements with regard to the matter of nuclear safety in Belarus. The institutions responsible for nuclear safety remain exposed to political pressure; the personnel of the NPP lack expertise and maintain substandard work ethics. Of note, Rosatom’s secondee Alexander Parfionov, the deputy senior engineer responsible for the nuclear safety at the NPP, resigned from his duties in the eve of the power start-up of the Belarus NPP.

Lithuania restricts electricity imports from the Belarus NPP under the law that forbids electricity imports from unsafe nuclear facilities. Nevertheless, Belarus maintains interest in trading its electricity in the Baltic market and thus seeks to bypass restrictions imposed by Lithuania via trading intermediaries, electricity swap schemes or transit via Russia.

Russia could altogether take over the operation of the Belarus NPP, as Belarus considers renouncing the rights to exploit the NPP and transferring them to a subsidiary company of Rosatom. This would further enhance Belarus’ dependence on Russia and make the power plant an entirely Russian project, as the latter already provided loans, nuclear fuel, and knowhow for the NPP.

Power start-up of the NPP is a phase when the NPP starts to produce electricity and the nuclear reactor’s power capacity is gradually increased to its intended capacity of its industrial exploitation.
RUSSIA MAY USE ITS NEW CARGO TRACKING SYSTEM FOR INFLUENCE OVER NEIGHBOURING STATES

Russia has created a new unified digital cargo tracking system, which is based on the Russian navigation system GLONASS. The Russian state corporation Rostech was one of the initiators of the project. GLONASS – managed by Roskosmos, another Russian state corporation – is the only navigation system permitted to use in the Russian Armed Forces. While GLONASS was originally created for the Russian military, its civilian use is intended as a cost covering measure.

Russia claims that installing electronic sensors into every vehicle used for transporting cargo will eliminate the need for any other type of inspection. These sensors consist of a locking seal and an electronic device used for tracking the cargo and monitoring the status of the seal. It is highly likely that one of the main reasons for developing such a system was Russia’s intention to gain control over all cargo transported among Russia, Kazakhstan, Belarus, China and the EU.

Data about cargo movement is provided to the Russia’s Federal Customs Service and Rostransnadzor, the Federal Service for Supervision of Transport. Digital Platforms Development Centre, while a subsidiary of RT-Invest Transport Systems, associated with the Rotenberg family close to Putin, operates the system.

Russia may exploit data from the tracking system as economic lever against businesses and states – for instance, in tailoring sanctions or advancing Russian business interests. There is also a risk that the tracking system will be used for data collection to meet the demands of the Russian Armed Forces.

CHINESE COMPANIES ARE INTERESTED IN DEVELOPING STRATEGIC IT INFRASTRUCTURE IN LITHUANIA

In 2020, a Lithuanian critical infrastructure company invited to tender for development of its smart IT infrastructure. The call attracted a lot of attention from Chinese entities, with one of them even offering to install the equipment.
free of charge in exchange for the system management rights. There were five enterprises with links to China among the potential supplier groups, with two of them jointly owned by the Chinese government. Entities associated with China were among potential suppliers of the equipment or technology, venture partners or subcontractors. It is likely that these entities were interested not only to develop their business ties, but also to gain knowledge on IT architecture in the domains critical to national security.

Chinese attempts to gain access to critical infrastructure reflect China’s overall objective to extend a long-term worldwide influence over strategic sectors and to establish their enterprises on the global markets. This would further enable China to advance dependency on its technology, to carry out intrusive cyber operations, including expropriation of data and knowhow, and would build its potential to undermine critical infrastructure in case of crisis.

Although Chinese enterprises suspended their investment plans in the container terminal in the port of Klaipėda, they maintained interest in other investment opportunities in Lithuania’s and other Baltic seaports, as it establishes a missing regional link connecting China’s land and sea transport corridors in its Belt and Road Initiative.

Countries under international sanctions are seeking ways to acquire strategic goods

Lithuania is handling considerable amounts of exports, including shipments of strategic goods – military and dual-use items. Dual-use goods are export-controlled as they can be used both for civilian and military purposes. This feature is often exploited by sanctioned countries that seek to acquire dual-use components to develop their weapons of mass destruction programs. Non-NATO countries often employ covert means to procure technology and equipment via shell companies to cover up acquisition schemes, for instance, by
using research institutes as their fronts. They may also try to take advantage of manufacturers that are not aware that third parties are intent to adapt their products for military use. Lithuania is committed to efficiently control movement of strategic goods to prevent entities under international sanctions from acquiring and using such items for domestic repression, violation of human rights, development of their military capabilities or weapons of mass destruction programs.
A LITHUANIAN CITIZEN PARTICIPATED IN THE ACTIVITY OF INTERNATIONAL ACCELERATIONIST GROUP

Over the past two years, the number of people supporting accelerationism, one of the most radical far-right ideologies, has increased in the West. The right-wing accelerationism is an extremist ideology which matured in the 2010s. Its adherents aim to demoralize society, undermine the democratic order and to replace it with white supremacy by means of violence, terror and guerrilla warfare. In the 1980s, James Mason, an American neo-Nazi ideologist, developed main ideas of accelerationism in his book ‘Siege’. In the following decades, the book became one of the principal sources of inspiration for accelerationists.

In recent years, supporters of accelerationism have committed many violent crimes, including murders, in many countries. Most of its followers are young – from 13 to 29 years old – and skilled in modern communications, including the use of online anonymity tools. Such skills allow them to exploit online tools for dissemination of propaganda, radicalization of others, sharing knowhow on making firearms or improvised explosive devices (IEDs).
In 2019, Gediminas Beržinskas, a Lithuanian citizen, was an active member of ‘Feuerkrieg Division’, an international accelerationist group. He created a large part of visual propaganda for the group and consulted its members on making and using IEDs. In October 2019, Beržinskas attempted to explode an IED outside the Western Union office in Vilnius. Another IED and an improvised firearm were found during an investigation of Beržinskas’ belongings. In September 2020, Beržinskas was convicted of an attempt to commit a terrorist act and of illegal disposition of firearms and explosive devices. He was sentenced to two years and four months of imprisonment.

‘Feuerkrieg Division’ operated for over a year. Several dozens of individuals from Europe and North America participated in its activities. The most active members faced court sentences or other preventive measures. There are currently no indications of the group’s continuing activity. However, new followers of right-wing extremist ideologies maintaining contacts with their foreign counterparts have been identified in Lithuania. Such individuals will likely aim to join new international groups of right-wing extremists.
What is radicalization?
Radicalization is a process of someone adopting an extremist worldview that motivates the individual to plot violent actions. Ideology is an important factor in the radicalization process that leads to terrorism. Individual political or religious beliefs and values alter significantly during the stage of radicalization. The individual may increasingly accept the use of violence as the only option to make the desired social and political changes.

Who is at risk?
A radicalizing individual aims to acquire a new identity proposed by the extremist ideology and propaganda. Persons of any age, social status or education can be radicalized – there is no typical model fitting all radicalization cases. Radicalization usually occurs within a social circle, whereas the Internet and social media accelerate the process. Young people are more susceptible to radical ideas, as narratives of extremist propaganda or the way of their presentation are specifically adapted to such audience.

What are the signs?
Radicalization can be difficult to spot because personal views change before any visual signs can be noticed. Ongoing radicalization can manifest itself in changing appearances, behaviour or rhetoric. Family members, friends and co-workers are usually the first persons to notice visual indications. However, visual indications do not necessarily mean a person is being radicalized.
**Interest:** the individual gets interested in the extremist ideology although visual signs (one’s appearances, behaviour or language) are covert or not yet noticeable.

**Radicalization:** the individual follows extremist propaganda online, adopts extremist worldview and does not hide it. The individual could be motivated by a perceived or genuine injustice or offence, a supposedly negative society’s attitude towards personal or group’s beliefs, a disappointment in politics or society and alienation. The individual might change one’s look and use certain symbols with the aim of belonging to the new social group and emphasizing differences between ‘us’ and ‘them’. The circle of friends changes, the individual becomes less social and breaks ties with friends and family.

**Indoctrination / extremism:** the individual spreads the extremist ideology, attempts to establish a closed radical social group or joins an existing one and attends its secret meetings. Such a radical social group provides a new identity and a status to the indoctrinated individual. Members of the group support each other’s views and radical positions. The individual tends to become aggressive and closed-minded, justifies and approves the use of violence as the only right way to problem solution. The individual approves the activity of terrorist organizations, may commit crimes or gets engaged in a criminal activity. One plans or threatens to use violence against an ‘enemy’ or a specific target and singles them out as the main cause of their problems. Signs of preparation to use violence may be evident, e.g. the individual participates in paramilitary trainings or special camps, seeks for information regarding IEDs or purchases weapons.

**Action / terrorism:** the radicalization process is over. One commits the planned act of violence and becomes a terrorist.
HOTBEDS OF TERRORISM POSE A SIGNIFICANT THREAT TO SECURITY OF EUROPEAN COUNTRIES

The terrorist organizations Islamic State of Iraq and the Levant (ISIL) and Al-Qaeda (AQ) continue planning attacks on Western targets and pose a major terrorist threat to European countries. Following some significant defeats, the ISIL has adapted to the new conditions and become a traditional underground terrorist organization using guerrilla tactics. The new leader of ISIL will highly likely aim to maintain a global network of loyal units, restore the ‘caliphate’ and continue the active anti-Western campaign. Although AQ, a rival of ISIL, has not been able to conduct any terrorist acts in Europe over the past five years, the group and its affiliates highly likely have been planning and seeking for possibilities to commit resonant attacks. The increasing activity and capabilities of AQ in the Middle East, Asia and Africa indicate the growing threat posed by this terrorist organization.

In 2020, international terrorist organizations failed to conduct coordinated attacks in Europe. However, there was an increase in individual attacks motivated by terrorist ideologies. There were 13 of such attacks in 2020 perpetrated in France, the United Kingdom, Austria and Germany. This trend indicates that radicalized individuals holding anti-Western sentiments continue plotting attacks in Europe. Their intent drives them to allocate personal resources to commit terrorist attacks even without maintaining ties with terrorist organizations.

The COVID-19 pandemic restricted the activity of local extremists in Europe. Restrictions on mass gatherings and events temporarily prevented terrorists from attacking crowds. Due to closed borders and restrictions imposed on public life, the movement of local supporters of extremist ideologies within the EU as well as the arrival of extremists from outside Schengen Area became complicated. Additionally, hundreds of terrorist fighters from Europe face difficulties to return from conflict regions in Syria and Iraq.
Extremists did not miss an opportunity to exploit the COVID-19 pandemic in order to boost their popularity. They used the pandemic for propaganda, to incite hatred and sow panic within societies. For instance, ISIL and AQ encourage exploiting coronavirus for bioterrorism, i.e. to spread the infection by coughing, spitting and other means, they refer to COVID-19 as God’s wrath upon the West. ISIL and AQ also incite their supporters to seize the opportunity and harder strike enemies that are supposedly less coordinated due to the pandemic. Due to the pandemic related isolation and social distancing, there is also a growing risk of self-radicalization, as more people are likely to come across radical and extremist materials online.
Terrorism threat in Lithuania is low. In 2020, the country did not receive any terrorist threats from abroad. Due to the movement restrictions within Europe and from outside Schengen Area, the possibilities for radical individuals to enter Lithuania also decreased. Although there were no identified organized Islamist and political extremism groups operating in Lithuania, radicalized individuals and lone actors continue to pose a risk.

STATES FACING CRISIS SEEK FOR PEACE BUT ENCOUNTER SERIOUS DIFFICULTIES

The agreement signed between the US and Taliban in February 2020 enabled the US to start their troops’ withdrawal from Afghanistan and contributed to strengthening the Taliban’s political and military positions. The most important issues related to peace and further state’s governing were, however, reserved for direct internal negotiations of Afghanistan. The talks officially started in September 2020, but they proceed very slowly. Despite negotiations, the Taliban is increasing military pressure on Afghanistan’s security forces by organizing attacks against them across the country. Accordingly, the security situation is deteriorating. Weak and fragmented Afghanistan’s government is dependent on international support and has few bargaining chips in negotiations. The Taliban is interested to wait until the foreign forces withdraw completely and to return to power either through negotiations or military force. Therefore, the ceasefire is unlikely in the short term.

The security situation in the Sahel region is deteriorating despite the increasing number of international military forces. Expansion of radical groups in the region is determined by their ability to establish themselves in local communities by taking advantage of the state’s inability to provide public services, poverty, ethnic and community conflicts. As military operations bring only a short-term effect and the state is unable to control large territories of the country,
Malian authorities consider negotiations with the most influential groups in the JNIM jihadist coalition. Instability in Mali in 2020 was also strengthened by a wave of political protests and military coup d’état in August. The transitional government that was formed by international agreement is also prone to negotiate with radical groups, though international partners conducting antiterrorist operations disapprove the idea.

In 2020, Iran intensified destructive activities aimed at forcing the US to leave Iraq. Iraq’s Shiite groups allegiant to Teheran regime actively organize attacks against the US diplomatic offices, US troops and logistic convoys. This poses a serious threat to the US and other foreign states’ troops and diplomatic personnel residing in Iraq. Iran’s actions negatively affect Iraq’s stability, complicate international community’s efforts to fight effectively against ISIL and thus create more favourable conditions for terrorists to operate.

The conflict in Syria has settled to a certain extent: the ceasefire agreed by Russia and Turkey has been present since March 2020. The level of violence in the country has decreased and stable front lines have been established. The
forces of the conflicting sides – the insurgents as much as the regime – were able to breathe a sigh of relief. Despite that, the ceasefire agreement provides only a temporary pause but does not ensure an enduring peace. The regime, however, does not hide their ambitions to regain all the lost territories, therefore, the vast scale military activities will highly likely resume in 2021.

ISIL shows no signs of strengthening or recovering neither in Syria nor in Iraq. Currently, the group has no intentions to control the territories again and is satisfied with the activity in the underground. ISIL fighters persist to be active and continue their terrorist attack campaign against civilian and military targets. The group will highly likely maintain the demonstrated operational pace in the short term. No major changes are expected in their activity.

The growing involvement of foreign states and military support for the conflicting sides had a critical importance for the course of Libyan conflict in 2020. Foreign aid to Tripoli government helped it to regain control of western Libya. The growing supply of modern equipment, aviation and mercenaries shows an increasing influence of foreign powers in the country but does not substantially change the strategic impasse. The need to end the oil blockade and international pressure induced representatives from different Libyan camps to announce ceasefire in October and resume the political dialogue with the UN mediation. However, it will take time and effort to finally implement the ceasefire agreement and form a unanimous state government. In the past, many of such attempts were simply unsuccessful. In case of failure, the risk that the armed conflict might resume will be high.

Intensified or resumed conflicts in states of the Middle East and North African regions would likely increase the flows of illegal migration to Europe.