REPUBLIC OF LATVIA
CONSTITUTION
PROTECTION
BUREAU

ANNUAL REPORT 2025

TABLE OF CONTENTS

DIGITAL VERSION OF THE REPORT

Egils Zviedris

Director of SAB

FOREWORD

The security situation in Latvia, the Baltic region and the world remains complex and does not give much reason for an optimistic outlook for the future. As assessed in our last public report, in 2025 a ceasefire in Ukraine was not achieved, despite various attempts. Russia continues its aggressive and confrontational approach towards Latvia and the West. The number of various sabotage and cyber incidents remains high.

A distorted threat perception continues to prevail in Vladimir Putin's regime, facilitated by the growing isolation of the Kremlin elite and lack of critical voices. Russia's perception of Western countries, including Latvia, is becoming increasingly aggravated and aggressive. The Constitution Protection Bureau (SAB) continues to obtain information confirming Moscow's increasing belief in its own propaganda where Europe, including Latvia, is depicted as a threat to Russia and its supposedly distinguished values. There is no indication that the Russian elite would change this view, even if peace in Ukraine were established.

Russia perceives offensive as the best defence, therefore it is trying to weaken the West both at the national and international level. Moscow's long-term goal is to dismantle the rules and rights-based world order and ensure that Russia is seen as a great power. In this report, we have highlighted how Russia's aggressive perception impacts all levels of decision-making, interweaving all areas of activity and economic sectors. Regardless of the outcome of the war in Ukraine and eventual peace agreement, the threat level stemming from Russia will remain high in the long term.

China also seeks to change the existing world order. China's strategy is based on purposeful identification and use of weaknesses, frequently hiding it behind seemingly positive initiatives and cooperation formats. Investments are often tied to economic dependency, scientific cooperation – with risks of technology transfers, use of Chinese technologies – with vulnerabilities in infrastructure of information and communication technologies (ICT), political and cultural cooperation – with expansion of soft power. We need to maintain a clear head and unified position at the national level as well as within the EU and NATO to efficiently resist the adverse effects of Chinese influence activities.

Year 2025 was also a significant one in the field of cybersecurity. Last year on June 25, the Cabinet of Ministers adopted a regulation aimed at

setting the minimum cybersecurity requirements – including for critical infrastructure in the ICT – which, in accordance with the National Cybersecurity Law, is supervised by SAB. This regulation is part of the legal basis which is being developed to form a cybersecurity framework corresponding to the current security challenges. The new regulation sets clear limitations, including a ban on cooperation with third countries (outside the EU and NATO), which government institutions must take into account during procurement procedures related to ICT resources, thus mitigating potential risks of malign influence.

Considering the above-mentioned and the upcoming Parliament elections, now, more than ever, it is important to demonstrate a unified approach and support to the democratic values on which the Latvian independence and state security is based. I encourage everyone, when consuming information, to be aware that we are under pressure from information influence activities. Our adversaries would certainly like to accomplish a large part of the work through the hands of Latvian people, without them even realizing it. Although invisible, this influence is very strong. It polarizes society and weakens national security. I would urge everyone to resist it in any possible way – do not give into emotions and fall for the traps set out in the information domain. It is always a good idea to take a deep breath before sharing seemingly scandalous information or drawing any conclusions about it, to not give our adversaries a reason to rejoice at the success of their influence operations which are aimed at undermining Latvian security and independence.

Taking a step back and looking at the larger picture, it becomes apparent that currently security is of the utmost importance. If we feel secure, we can live, strive for and achieve our goals, and celebrate our achievements. We can do the mundane tasks and enjoy the small – yet so important – moments of happiness. We often think and appreciate things and values once we face a threat of losing them. Therefore, at the turn of the year, when we tend to set goals for the next one, I would like to remind you – let us always plan and make decisions which serve the interests of Latvian security. National security is not something that can be provided to us solely through the work of the government or security agencies. It is the result of our common efforts and daily investments. Let us be united and work together for a secure and independent Latvia, in every choice and action keeping in mind that it is an honour to serve Latvia and a necessity to strengthen our home.

EGILS ZVIEDRIS

Director of SAB

EXECUTIVE SUMMARY

In 2025, Russia's full-scale invasion and its consequences continued to impact the security and prospects in Latvia and other Western countries.

Even though, since the beginning of 2025, discussions on potential peace talks between Russia and Ukraine have periodically appeared on the international agenda, our information indicates that Moscow is prepared to continue hostilities also during 2026: Russian military tactics, economy, and society are being increasingly adapted to long-term hostilities.

The current state of Russia's war against Ukraine can be characterised by intense fighting, with neither side gaining a decisive and strategic advantage. Despite Moscow's advantage in terms of military resources and soldiers, Ukrainian army has sufficient military capacity to prevent a strategic-level Russian breakthrough. Both sides have adjusted their tactics – enhancing actions aimed at exerting pressure and tiring the other side, while reducing the loss of their own resources.

If these trends persist, there is a very low probability of any strategic-level changes on the front line over the next six months. Therefore, it is very likely that Russia will try to achieve its maximalist goals regarding Ukraine by using potential peace talks and international pressure, including attempts to reduce Western military support for Ukraine.

Russia continues to focus on militarization of its economy, achieving current economic stability and resilience to Western sanctions at the expense of long-term prosperity. The rapid redistribution of resources and unequal support across various economic sectors is creating a structural imbalance that will likely have negative consequences in the future. As things stand, there is a low chance of the Russian economy collapsing in the short term; however, the country's technological development and international competitiveness will decline in the long term.

In our assessment, the militarization of the Russian economy will continue even after a potential conclusion or freezing of the war in Ukraine: Russia will further develop its military capabilities, continuing to pose a significant threat to European countries and NATO. In addition, a potential conclusion of the war resulting in Western countries lifting or easing the sanctions imposed on Russia would notably increase Moscow's ability to maintain a high level of economic militarization without having

to put up with the risk of a significant economic turmoil.

Over the past few years, Moscow's perception of the West as an existential threat to the ruling regime has only intensified. Putin's regime continues to have a distorted threat perception, facilitated by the growing isolation of the Kremlin elite and lack of critical voices. Russia believes it has already entered a direct confrontation with the West: the struggle takes place not only in Ukraine, but also globally and ideologically.

This worldview increases various risks of miscalculation. Russia's aggravated threat perception means a significant increase of security threats for Europe. In 2025, Russia continued to deploy a wide range of instruments of influence against the West to undermine Western unity in supporting Ukraine or even to achieve a potential cessation of this support and prepare for a potential confrontation with NATO. Russia continued to conduct not only sabotage and information activities against Western countries, but also its readiness to carry out cyber attacks on industrial control system in Latvia and Western countries, which can lead to both short term inconveniences and threats to security of critical infrastructure. The aim of these activities is to spread uncertainty and mistrust among the population, undermine the quality of services, punish for supporting Ukraine, and discourage from showing support in future.

The use of legal mechanisms in the international arena became increasingly widespread. Russia mostly uses legal instruments by referring to international norms allegedly violated by the West, including Latvia. This is done via various platforms – international organizations, official statements, and propaganda narratives. In its propaganda messages, Moscow likes to emphasize the alleged double standards of the West, while portraying itself as a constructive actor that adheres to international norms.

Russia pays particular attention to the United Nations (UN). For the past year and a half, the Russian Ministry of Foreign Affairs has been periodically reporting that it is preparing to sue the Baltic states, including Latvia, as well as several other countries at the UN International Court of Justice (ICJ) regarding violations of the Russian-speaking residents' rights. The aim of litigation – to discredit Latvia on an international level and ensure a long-term international pressure on Latvia to change its policy towards Russia and the Russian-speaking population.

The example of Belarus demonstrates that a close cooperation with Russia only increases the intensity of Moscow's influence activities. The political cooperation between the two countries continues to develop with Russia's growing structural influence over Belarus. Both countries

are undergoing a gradual and institutionalized integration process within the Union State comprising virtually any area of policy. Our information indicates that Moscow has a sensitive perception of even the smallest efforts by the Belarusian regime to implement a more independent policy. Since Russian invasion of Ukraine, the economic cooperation between Russia and Belarus has become increasingly militarized, with more and more Belarusian companies re-profiling their activities and production to meet the needs of the Russian military-industrial complex. In case of a military conflict, the civilian economy of Belarus will also fully serve Russia's military interests.

China also expands its political influence in Western countries and international organizations and uses various types of investment to create economic influence (and dependence). Beijing uses soft power activities to create a positive image of China in Western society. Academic and scientific cooperation projects are used to access sensitive information and share the acquired knowledge and technologies without permission, or to develop contacts to advance China's economic and military superiority in regard to other countries. We would like to remind students and researchers to be vigilant and carefully evaluate potential cooperation projects and study exchange opportunities to limit the transfer of knowledge and technology to other countries.

RUSSIAN INVASION OF UKRAINE

The full-scale invasion of Ukraine has lasted for almost four years, and our information indicates that Russia is ready to continue hostilities well into 2026. Military tactics, the economy, and society are increasingly being adapted to a long-running conflict. Both at the front line and in the context of potential peace talks, Moscow continues to demonstrate that it has not abandoned its maximalist goal – returning Ukraine to Russia's perceived sphere of influence.

In the Russian war against Ukraine, there is currently intense fighting, with neither side gaining a decisive advantage. Despite Moscow's predominant military resources and soldiers, Ukrainian army has sufficient military capacity to prevent a Russian breakthrough at a strategic level. Even though Russian troops have maintained the initiative along the entire front line since the beginning of 2025, advancement into Ukrainian territory is proceeding rather slowly: Moscow's control over Ukrainian territory has increased by approximately 0.4–0.7% in 2025. The relatively small territorial gains have come at a high cost for Russia: the number of seriously wounded and killed soldiers (over 25 000 per month) is close to the number of soldiers being mobilized (30 000 to 35 000 per month). The need to replace the fallen and wounded soldiers limits Russia's ability to prepare for a larger-scale attack.

The development of drone technology is becoming a very important element in the current phase of the war. Various types of drones are responsible for 70 to 80% of the killed and wounded soldiers in both the Russian and Ukrainian army. Their widespread use allows both sides to conduct reconnaissance, artillery fire correction, and strikes on enemy troops and equipment. Unmanned systems largely determine the effectiveness of offensive and defensive operations. This development of hostilities has caused both sides to adjust their tactics – enhancing actions that exert pressure and tire the other side, while reducing the loss of their own resources, e.g., by intensifying the use of drones or small infiltration groups of a few people instead of massive attacks. This makes the war more dynamic at the tactical level, but reduces the chance of either side making a strategic breakthrough.

Due to the above-mentioned factors, both sides have been focusing on the development of long-range attack capabilities. In January 2025,

Russia launched an average of 85 Shahed drones per day against Ukraine, whereas in November the number had already increased to 170–190 drones per day. Ukraine has also significantly intensified drone strikes on military and energy facilities in Russia, with a particular emphasis on precision and psychological impact. For example, during the operation SpiderWeb in June 2025, truck-launched drones attacked four military bases, the most remote of which were located several thousand kilometres from the front line.

If these trends continue, there is a very low probability of any strategic-level changes on the front over the next six months. Therefore, it is very likely that Russia will try to use potential peace talks and international pressure, including attempts to reduce Western military support for Ukraine, to achieve its maximalist goals regarding Ukraine. Thus, it will be Western military and political support that will largely determine Ukraine's ability to resist Russian aggression.

MILITARIZATION OF THE RUSSIAN ECONOMY

The full-scale invasion of Ukraine has contributed to a significant militarization of the Russian economy, shifting its main focus to meeting the needs of the army. Over the next three years, Moscow plans to allocate 38–41% of budget expenditures, or over 6% of GDP, to military needs. The current growth of the Russian economy is largely due to large investments in the military-industrial complex. In our assessment, the militarization of the Russian economy will continue even after a potential conclusion or freezing of the war in Ukraine. We also expect further development of Russian military capabilities, which will create a significant threat to European countries and NATO. In addition, a potential conclusion of the war resulting in Western countries lifting or easing the sanctions imposed on Russia would notably increase Moscow's ability to maintain a high level of economic militarization without having to put up with the risk of a significant economic turmoil.

Since the invasion of Ukraine, Moscow has demonstrated a constant ability to adapt to the constraints imposed on it. Russian economy has become an indicator of both its prosperity and future security policy. Russia continues to shift the focus of its economy towards militarization, achieving current economic stability and resilience to Western sanctions at the expense of long-term prosperity. The significant allocation of resources to arms production together with efforts to improve and develop self-sufficiency in military production mean that Russia will continue to pose a military threat to its neighbours in the future.

Although Russian officials have tried to reduce the impact of hostilities on the daily lives of the population, changes to the Russian economy and society have been significant and present since the beginning of the war. While the massive spending and influx of resources into the military-industrial complex currently support Russian economy, the civilian sector faces declining activity and lack of development prospects caused by sanctions, the growing tax burden, as well as limited and expensive access to capital. The rapid redistribution of resources and unequal support across economic sectors is creating a structural imbalance that will likely have negative consequences in the future. As things stand, there is a low chance of the Russian economy collapsing in the short term; however, the country's technological development and international competitiveness will decline in the long term.

The Russian military-industrial complex is operating at full capacity: arms production is carried out in multiple shifts and investments are made in factory expansion and accelerated acquisition of new capabilities, such as drone production. This, combined with the use of its historical industrial base, has allowed Russia to expand arms production in 2025, relying on the principle of quantity over quality.

Nevertheless, Russia has faced certain shortcomings in the military-industrial production, such as reliance on foreign imports, and limitations in the available labour force and production capacity. The shortcomings are partially addressed by financial resources. Russia's plans for the federal budget over the coming years indicate an almost unchanged commitment to continue arms production and expand the capabilities of the military-industrial complex.

The war and the militarization of Russia's economy have created a circle of political and economic stakeholders who benefit from the war, posing an additional obstacle for a potential reduction of military spending and militarization in the future. The demand for arms production remains consistently high, and the industry, comprising more than six thousand companies directly or indirectly involved in the Russian economy, contributes to further dependence on high military spending.

Given the need to restore its war-depleted arms reserves as well as the importance of military production for the economy, Russia will keep its economy militarized even after the end of the war in Ukraine. It is very likely that Moscow will gradually reduce its military spending to lower the risks of economic instability and restore its military capabilities. Despite Russia's expanded military production being technologically relatively simple, the ongoing militarization of the country's economy will still pose a threat even after the war in Ukraine ends.

RUSSIAN REGIME'S PERCEPTION OF THE WEST AND THE BALTICS

The Russian war in Ukraine demonstrates that Moscow is capable of making important strategic decisions, like invading a neighbouring country, based on a distorted threat perception and assumptions that are detached from reality. In 2022, Putin's regime believed that, faced with military superiority, Ukraine would surrender and Western countries would not be ready to provide Kyiv with military and financial assistance. In our assessment, Putin's regime will continue to have a distorted threat perception in 2026, facilitated by the growing isolation of the Kremlin elite and lack of critical voices. Russia's perception of Western countries, including Latvia, is becoming increasingly aggravated and aggressive, which can contribute to increasingly aggressive Russian activities in the long term. NATO's deterrence capabilities and strategic communication play a crucial role in reducing and even preventing Russian aggression. Potential security risks could be significantly reduced by sending Russia a clear message to avoid any provocations or aggressive actions and pointing out the consequences of such actions.

Moscow's perception of the West as an existential threat to the ruling regime has only intensified since the invasion in 2022 and the following Western support for Ukraine. Russia believes that it has already entered a direct confrontation with the West and that the West is supposedly trying to destroy it. Moscow sees the struggle as taking place not only in Ukraine, but also globally and ideologically. Russia assumes that Western values, such as democracy, civil society, and human rights, would weaken the regime's control over the country and thus pose a threat to its stability.

Russia's heightened threat perception is also enhanced by its view of international developments as a zero-sum game. Russia often interprets the actions of other countries in terms of resemblance, assuming that they are going to act in the same way as Russia would in a similar situation. Moscow views countries that are favourably inclined or at least neutral towards Russia as part of an existing or potential new coalition against the West, based on the "West versus the rest" idea.

Consequently, Russia aims to weaken the West at the national and international level and transform the European security architecture in the long-term. This worldview increases the risks of miscalculation. Intensified Russian perception of threats means significantly increased security risks for Europe. Russia is often fighting or preparing to fight imaginary threats, for

example, when it started escorting the "shadow fleet" tankers in the Gulf of Finland due to concerns about aggressive actions against them, or when, following NATO' s response to Russian drones entering Polish airspace on 10 September 2025, the Russian Ministry of Foreign Affairs warned that it would shoot down objects in Russian airspace. All of this makes Russian activities increasingly unpredictable – it is markedly more difficult to assess potential actions from the perspective of objective reality.

Our observations show that Russia's perception of Latvia is becoming increasingly similar to the one Russia had of Ukraine before the war. While Russia does not pose a direct military threat to Latvia at the moment, a number of signs indicate potential long-term plans. Our information indicates that Russian officials believe the propaganda the regime has created and disseminated about Latvia. Although not a priority for Russia, the increasingly negative view of Latvia may result in more aggressive Russian decisions in the long term.

Most Russian narratives portray Latvia as a russophobic country that oppresses the Russian-speaking part of the population. The Russian Ministry of Foreign Affairs periodically publishes voluminous reports on human rights violations and the situation in Western countries, quite often dedicating one of the biggest parts of the report to Latvia. Russian narratives also depict Latvia as a Nazi state, a puppet of the Great Britain and the United States, and a failed state. Before the war, Moscow was spreading similar narratives regarding Ukraine. Now, it continues to portray all three Baltic countries in a similar way.

Russia secures the stability of the regime through repression

The stability of Putin's regime is considered a priority among Russian perception of domestic threats. The ruling regime views any public discontent and protests as initiated or at least supported by the West. The Kremlin tries to limit the spread of any undesirable sentiments by using the regime-controlled media to disseminate military-patriotic propaganda narratives and increasingly restricting the population's access to alternative information. To prevent public dissatisfaction from turning into political alternatives or mass protests, Russia continues widespread repressions against the opposition and society in general. According to our information, in the coming years Russia is going to intensify repressions and state control over the media, at the same time reducing the availability of information that is not controlled by the regime.

The political and economic elite as well as the power structures supporting the regime are essential for the domestic stability. Moscow maintains this support by offering opportunities for personal gain and retaining fear of repression among these groups.

RUSSIAN ATTEMPTS TO DISRUPT WESTERN UNITY

In 2025, Russia continued to deploy a wide range of influence instruments against the West to undermine (or even end) Western unity in supporting Ukraine and prepare for a potential confrontation with NATO. However, Moscow's main priority remains victory in the war with Ukraine. This means that Russia must subordinate its economy and other government functions to the needs of the war, thus limiting the ability to escalate activities towards the West.

For Moscow, Western support to Ukraine (be it military, financial, or other) means that the war with Ukraine is perceived as a broader conflict between Russia and the West. Kremlin uses various hybrid instruments to promote war fatigue and intensify (or create new) rifts among and within Western countries. By doing so, Moscow hopes to reach a critical mass to reduce, if not stop, the military support to Ukraine and exert political pressure on Kyiv to sign an agreement with Russia.

Sabotage activities

Russia is constantly looking for weaknesses in Western security that could be exploited in the future. In 2025, Russia continued to expand sabotage activities, mostly targeting infrastructure used to provide military support to Ukraine. We have seen continuous cases of GPS signal jamming and spoofing in the Baltic Sea region, which could be explained by Russia conducting protective measures against drone attacks and concealing the activities of its "shadow fleet", as well as causing additional disruptive effects on air and ship traffic of NATO member states.

In 2025, there has been an increase in airspace violations and the number of unidentified drones being observed over NATO member states, including critical and military infrastructure. Russia has used the disruptions caused by drones to the airports in its information activities, highlighting the vulnerabilities of European countries, e.g., the inability to control airspace.

Regardless of whether Russia is responsible for the incidents or not, Moscow is closely monitoring the Western response to the various security incidents (drone flights over airports, sabotage of critical infrastructure facilities, etc.).

Information activities

Moscow continued to influence both Latvian and international information domain, spreading narratives that are in line with Russian interests. These narratives aim to increase discord and differences in Latvian society and reduce trust in government institutions and our allies in the EU and NATO. Russia constantly tries to discredit Latvia internationally. Social networks and communication applications are gaining increasing importance for the dissemination of Russian narratives.

Information influence activities were also one of the main tools Russia used when trying to manipulate elections in Europe in 2025. Moscow used fake social media accounts to spread support for candidates preferred by Russia, while disseminating defamation for candidates who embraced the European course and advocated for continuous or even increased support for Ukraine. Information influence activities were also used to reduce public trust in the electoral process and democracy in general.

We also observed an increasing use of artificial intelligence (AI) in Russian information operations to generate content that is more suitable for target audiences and easier to understand. AI can also reduce the cost of creating content in other languages and distributing it outside traditional Russian target groups.

Russian diplomats are also involved in information activities, spreading narratives about Moscow being open to dialogue and Western countries – especially NATO members – escalating the situation. We would like to particularly highlight Russian officials criticising NATO's allegedly aggressive actions in the Baltic Sea.

Exploitation of economic and energy relations

Although the EU is constantly working on decreasing its economic and energy dependency on Russia, Moscow seeks ways to use its economic potential and energy resources to maintain influence. Russian officials regularly highlight the importance of Russian energy and other raw materials for the global economy and vast opportunities that would be opened up by renewed cooperation. Russian representatives have also emphasized this economic potential in negotiations with the United States within the framework of the Russia-Ukraine peace process. Furthermore, Moscow is trying to use a more favourable pricing policy for gas (including liquefied natural gas) and oil in relations with Europe. Despite Russia's deteriorating economic performance, we can still see that, internationally, Moscow is using the Russian domestic market as an argument to attract other countries capable of satisfying this market's demands.

It is very likely that Moscow's continued war against Ukraine, combined with the regime's perception of its supposedly existential conflict with the West, will lead to increased intensity of hybrid activities in the coming years. The high risks related to an open military confrontation with NATO will likely result in predominantly covert hybrid operations, for example, sabotage, cyberattacks, information operations, and a wider integration of AI capabilities into influence campaigns. Western countries gradually diversifying their energy supplies and reducing their dependence on Russia will most likely result in Moscow increasingly turning to sanction-circumvention schemes, proxy states, and cooperation with authoritarian partners.

INTERNATIONAL LEGAL MECHANISMS AS RUSSIA'S NEW HYBRID TOOL

Since the full-scale invasion of Ukraine in 2022, Moscow has been constantly adapting existing and creating new hybrid instruments for its imagined fight against the West, including international legal mechanisms. Our information indicates that the Russian Ministry of Foreign Affairs has internally acknowledged that Russia is required to take legal action against the West in international organizations and courts because of the alleged legal warfare supposedly taking place between the two sides. In the long term, Moscow plans to use this hybrid instrument to eliminate the rules-based world order and ensure that Russia is perceived as a great power.

Russia mostly uses legal instruments to refer to international norms allegedly violated by the West, including Latvia. This is done via various platforms – international organizations, official statements, and propaganda. In its propaganda narratives, Moscow emphasizes the alleged double standards of the West, trying to portray itself as a constructive actor that adheres to international norms.

Russia pays particular attention to the United Nations (UN). According to our information, Moscow believes it to be the right platform for achieving beneficial short-term decisions and long-term geopolitical changes. Russia's current priorities include legitimizing its aggression in Ukraine and securing at least a neutral position from other UN members on the issue. Even though the vast majority of UN members have so far condemned Russian aggression, this trend is changing, and Russia is strengthening its positions. Moscow's influence in the UN is determined by its special status: Russia has veto rights in the UN Security Council, the organization's most influential body, which determines international sanctions policy. Russia uses this status to gain the neutrality or even favour of other countries on issues important to it.

From words to actions: Russia plans to sue Latvia at the UN International Court of Justice

In 2025, Russia intensified legal warfare against the West, particularly the Baltics. For the past year and a half, the Russian Ministry of Foreign Affairs has been periodically reporting that it is preparing to institute proceedings against the Baltic states as well as several other countries at the UN International Court of Justice (ICJ). In May 2025, Russia announced that it is preparing an application to be submitted against the

aforementioned countries at the ICJ. It is very likely that the preparation process is in its final phase, and Russia will file the application against Latvia in 2026.

Russian accusations are based on the usual theses about violations of the Russian-speaking residents' rights. Russia accuses Latvia of violating the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), stating long-standing discrimination against Russians and Russian-speakers, non-citizen status, elimination of Russian cultural and historical identity, education in the Russian language, etc.

Russia wants to use the case against Latvia to discredit our country internationally and ensure long-term international pressure that would force Latvia to change its policy towards Russia and the Russian-speaking population. The case against Latvia might also be used to justify Russia's increasingly aggressive activities against the Baltic states in the information domain. It is very likely that Russia will use the accounts of various pro-Russian activists and other people who have moved to Russia in its accusations against Latvia at the UN ICJ.

Russia's main accusation against Latvia: violations of the rights of the Russian-speaking population

While preparing the case against Latvia for the ICJ, Russia simultaneously continues to discredit our country, claiming that Latvia violates international obligations and openly targets the Russian-speaking population. The Russian Ministry of Foreign Affairs periodically publishes various reports on the human rights situation abroad, and Latvia is often given one of the largest chapters. In 2025, Russia actively used legal arguments in issues related to amendments to the Latvian Immigration Law regarding Latvian language proficiency tests.

Moscow often discredits Latvia based on the opinions of pro-Russian activists and people who have moved to Russia. The Kremlin's propaganda constantly features stories of people who have moved to Russia and complain about russophobia, decline of traditional values, closure of Russian-language schools, and the poor economic situation in Latvia.

Russian compatriot organizations are also conducting information influence activities aimed to (internationally) discredit Latvia. The Foundation for the Support and Protection of the Rights of Compatriots Living Abroad is one of the main organizations expanding their influence activities against the Baltic states. Supervised by the Russian Ministry of Foreign Affairs, it regularly finances the services of lawyers for pro-Russian activists being tried in Latvia or abroad. These cases are usually widely covered by Russian propaganda and official rhetoric.

RUSSIA-BELARUS RELATIONS

Russia's long-term goals in Belarus: determined by Moscow's perception of threats

The political cooperation between the two countries continues to develop in line with Russia's growing structural influence over Belarus. The gradual and institutionalized integration into the Union State is affecting virtually every area of policy. In the medium to long term, Russia wants to achieve full control over political processes in Belarus, thus reducing the risk of any unplanned changes in the Belarusian regime that could lead to potential changes in its foreign policy.

The Union State and its integration programs provide the most important cooperation platform between the two countries, allowing Russia to structurally strengthen its influence over Belarus. Referring to the Union State agreements, Ministries of Foreign Affairs in both countries continued to coordinate most foreign policy issues in 2025, including relations with Western countries and Ukraine, as well as their positions in international organizations. Moscow uses these consultations to ensure Belarusian foreign policy stays in line with Russian interests, thus making it into a continuation of Russian foreign policy. In 2025, we also saw continuous integration programs for taxation, customs, and financial markets, as well as production, agriculture, education, and regional cooperation.

Our information indicates that, despite Russia's growing influence over Belarus and its pronounced pro-Russian course, Moscow is becoming increasingly sensitive in its perception of even the smallest efforts by the Belarusian regime to implement a more independent policy. For example, Russia sees Belarusian return to economic cooperation with European countries as contributing to Lukashenko's multi-vector foreign policy which automatically reduces Russian influence over Belarus. A potential replacement of Lukashenko's regime, without a prior coordination with Russia, would be perceived by Moscow as a threat to Russia and its interests in Belarus.

Russia almost certainly wants to create a situation where structural dependence of the country will force the next Belarusian leaders to continue a strong pro-Russian course, both domestically and internationally. The integration process of the Union State is generally going well and will continue to promote Russia's structural influence. At the moment, Moscow has no direct influence over Lukashenko's domestic policy; still, both sides want to

prevent political instability similar to the 2020 protests, which would be seen by the Kremlin as a threat to its interests. Moscow will most likely suppress any efforts by Lukashenko's regime to restore relations with European countries, if it does not benefit Russia.

Economic cooperation between Russia and Belarus becomes increasingly militarized

Since the Russian invasion of Ukraine, the economic cooperation between Russia and Belarus has become increasingly militarized, with more and more Belarusian companies re-profiling their activities and production to meet the needs of the Russian military-industrial complex. Belarusian companies supply Russia with dual-use and ready-made military products. It is almost certain that the mutually beneficial economic cooperation between Russia and Belarus will continue in the future.

Around 500 Belarusian companies are integrated into the military production system, receiving state subsidies for re-profiling of the production[1]. Most of the re-profiling is done by companies with previous experience in the production of dual-use products, like microelectronics, optical products, chemicals, or large-sized trucks. These Belarusian manufacturers use their logistics networks to help supply the Russian military-industrial complex with components manufactured both in Western countries and elsewhere.

More and more Belarusian companies take advantage of Russia's growing demand for military products that can be used immediately in the war in Ukraine. Russia is considering the possibility of building a drone production plant in Belarus with the annual capacity of up to 100 000 units. Each year, Belarus provides Russian missile launchers with around 480 000 artillery and rocket shells, using the production equipment supplied by China.

The war in Ukraine shows that in case of a military conflict, the civilian economy of Belarus will also fully serve Russia's military interests. Minsk almost certainly sees the provision of military-industrial assistance as the best way to support Russia in the war with Ukraine. It allows Belarus to avoid a direct engagement in the hostilities, while providing economic and financial benefits for Lukashenko's regime. If the Kremlin maintains its aggressive foreign policy towards the West, Belarus will, most likely, have an increasingly important role in Russia achieving not only its military but also military-industrial goals.

[1] According to research by the Belarusian opposition organization BelPol.

CHINESE ATTEMPTS TO GAIN INFLUENCE IN THE FIELD OF SCIENCE

China's main priority is to establish itself as a global economic and military power. To achieve this, Beijing is developing comprehensive activities aimed at promoting domestic growth and strengthening its positions externally. China is expanding its political influence in Western countries and international organizations both in open and covert ways, using various types of investment to create economic influence (and dependence), as well as soft power activities to create a positive image of China in Western society.

Chinese Communist Party's military-civil fusion strategy is one of the instruments Beijing uses to strengthen its domestic and external positions. The strategy envisages the establishment of close cooperation between China's defence and military structures, as well as civilian actors, including science and technology institutes, educational institutions, and research centres. These actors are constantly working to identify weaknesses, eliminate shortcomings, and create innovations that would lead to economic and military superiority over other countries.

To effectively achieve these goals, China is constantly trying to obtain information on its competitors and learn from their achievements. Information is often obtained through various academic and scientific cooperation opportunities, such as student exchange programs, joint projects, and foreign researchers working in China. It is important to note that China's legislative framework stipulates that every citizen is obliged to help the state achieve its strategic goals. This obligation includes providing security services with all the required information. It also applies to the academic and scientific environment. Representatives of these fields can use projects abroad to access sensitive information and share the acquired knowledge and technologies without permission or develop contacts that could provide useful information in the future.

Risk groups for cooperation with China

Although all Chinese citizens are required to cooperate and share information with Chinese state bodies, certain groups pose additional risks in the field of science. They include 1) individuals who have studied or are currently studying/working in the field of sensitive technologies, 2) individuals who belong to Chinese universities subordinated to defence and security services, and 3) individuals who receive Chinese state scholarships.

1. China aims for more than just catching up with other great powers, such as the United States or the EU; it wants to surpass them, ensuring permanent dominance. This is why China intends to advance emerging and disruptive technologies. By successfully developing these technologies, Beijing can gain complete dominance in a given sector and prevent competitors from gaining an advantage. Particular attention should be paid to cooperation projects with Chinese citizens that include the following emerging and disruptive technologies: artificial intelligence, quantum technology, renewable energy, biotechnology, medicine, space technology, and robotics. It should be noted that both Chinese citizens and citizens of other countries with knowledge of these technologies and their development in the West may be subject to interrogations, searches, and even recruitment by Chinese security services.
2. Risks are also posed by individuals who belong to Chinese universities operating under the supervision of or receiving funding from Chinese defence and state security services. The greatest risk is posed by the so-called "Seven Sons of National Defence" – seven universities historically associated with the Chinese defence sector, which still spends about half of their budget on defence projects. In addition, more than 60 universities subordinated to the State Administration of Science, Technology and Industry for National Defence are directly responsible for the implementation of the aforementioned military-civil fusion strategy. Cooperation with representatives of these universities may create risks of knowledge and technology transfer, whereas the products created during such cooperation might be used in China not only for civilian, but also military purposes.
3. China promotes international cooperation in the field of science through various support programs, including scholarships offered by the China Scholarship Council. These scholarships pose high counterintelligence risks, as their recipients are often subject to various conditions, e.g. the obligation to maintain regular communication with the Chinese embassy in the respective country or reporting on their study progress, achievements, and established contacts. The students are also often required to work in China for several years. Consequently, there is a risk that, in order to fulfil the conditions of the scholarship, the jointly developed technologies and acquired knowledge may have to be leaked to unauthorized persons.

Mitigation of risks

SAB is taking steps within its mandate to limit the aforementioned risks. We are one of the institutions that evaluate visa applications of foreign

citizens. To reduce potential risks to the academic environment, visa applications from Chinese students and researchers are subject to particular scrutiny. SAB carefully evaluates the educational institution from which the visa applicant graduated, their previous field of study, and any support the Chinese government may have granted them. Upon identifying a set of factors that may pose risks to national security, we issue a recommendation to the responsible authorities to refuse the visa in the particular case. To limit the access of knowledge and technology by competing countries, SAB has also developed a targeted cooperation program with universities and scientific research institutes. We encourage educational institutions to use publicly available resources to check the connections of their foreign partners for cooperation with the defence sector of their respective parent country, e.g. China. Before starting the cooperation, scientists and researchers are also encouraged to verify whether the final product cannot be subjected to any export control bans. In addition, we offer briefings to academic personnel about the security and intelligence risks associated with collaboration offers that involve travelling to China, e.g. digital security and potential recruitment.

We would like to urge all students, academic personnel, and researchers to be vigilant and carefully evaluate any potential collaboration projects and study exchange opportunities. While sharing of knowledge and development of new skills are certainly natural and necessary components of science, they can also pose risks for both the expert themselves and the country they represent. Each case must be carefully assessed to ensure that the potential benefits promised by the foreign partners, such as funding, equipment and technology, outweigh the potential risks and losses.

CYBER THREATS

The overall level of registered cyberthreats towards Latvia reached an all-time high in 2025, having increased multiple times since Russia's full-scale attack on Ukraine in 2022. Most of the cyber incidents were cyber crimes and various types of digital fraud, which rarely threatened critical infrastructure or national security interests.

In 2025, SAB assessed the threat level posed by cyber actors of hostile states to Latvia as still elevated. Similarly to previous years, the activities of hostile cyber actors varied in intensity, they were not constantly high or linearly increasing. Most of the observed cyber-attacks had very limited negative effects. This was largely due to the successful prevention and effective reaction by the defenders of the Latvian cyber domain.

Latvia experienced a full spectrum of cyber-attacks in 2025. From the national security perspective, the most significant threats included intrusion attempts, malware distribution, compromising of equipment, and distributed denial-of-service attacks.

Russia continued to pose the main cyber threat to Latvia due to Russian strategic goals in general as well as the military, political, and other types of material and psychological support Latvia provided to Ukraine in its defensive efforts against Russia.

SAB continued to observe a trend that started in 2024: large, public, and politically significant events not attracting any cyber-attacks of hostile states. In 2024, Latvia did not experience significant cyber-attacks during the European Parliament elections and the Parliamentary Summit of the International Crimea Platform in Riga. Similarly, in 2025, we did not observe any external, hostile cyber-attacks during the local municipal elections. It can at least partly be explained by the preventive defensive measures, especially efforts by the national Cyber Incident Response Institution – CERT.LV.

Cyber threats to operational technologies were also a cause for growing concern. Operational technologies are equipment and software used to monitor and control physical processes, devices, and infrastructure to provide, among other things, essential public services – energy, water supply, and transport. Despite the ever-increasing number of devices that is nowadays managed remotely, in many cases, these systems are lacking the necessary level of cyber security. That, in turn, allows malicious cyber

actors to use relatively simple methods to gain remote access to industrial control systems or other operational technologies, allowing them to disrupt essential services. According to ENISA, almost one fifth (18.2%) of the cyber-attacks in Europe were targeted at operational technologies.[2]

Russian hacktivists[3] have shown that they are willing and capable of carrying out cyber-attacks on Latvian and Western industrial control systems, designed to create short-term inconvenience or even threaten the security of critical infrastructure. Hacktivists aim to affect vital services, shock, sow doubt among the general population, punish for the support previously provided to Ukraine, and deter from providing any support in the future. For instance, in April 2025, Norway experienced a cyber-attack against a dam on the Risetvatnet lake. Russian hacktivists exploited a weak password to gain access to a control panel that was connected to the internet and regulate the dam's minimum water pass-through. Attackers increased the water pass-through, which was only noticed four hours later. Luckily, the water level did not drop to a critical level, and the dam in question was used for fish farming instead of, for example, supporting the operation of a hydro-electric power plant. In August 2025, Russian hacktivists repeatedly attacked the Gdansk hydro-electric power station. During the second attempt they managed to remotely access control systems and change operational parameters. As a result, they caused the generator and rotor to stop, which lead to a full shutdown of the power plant.

Thus far the vulnerabilities of Latvian operational technologies have mostly been discovered through preventive cyber security measures and monitoring. Significant incidents endangering critical infrastructure and vital services have not been registered. For example, in 2025, as part of monitoring activities, it was identified that the software and applications used in a municipal service provider's industrial control systems and service provision were highly vulnerable to potential attacks via remote access. Observations regarding critical infrastructure and essential or important service providers show that all of them need to constantly improve the cybersecurity of their operational technologies and systematically implement measures, procedures, and technical solutions to minimize the negative impact of potential cyber-attacks.

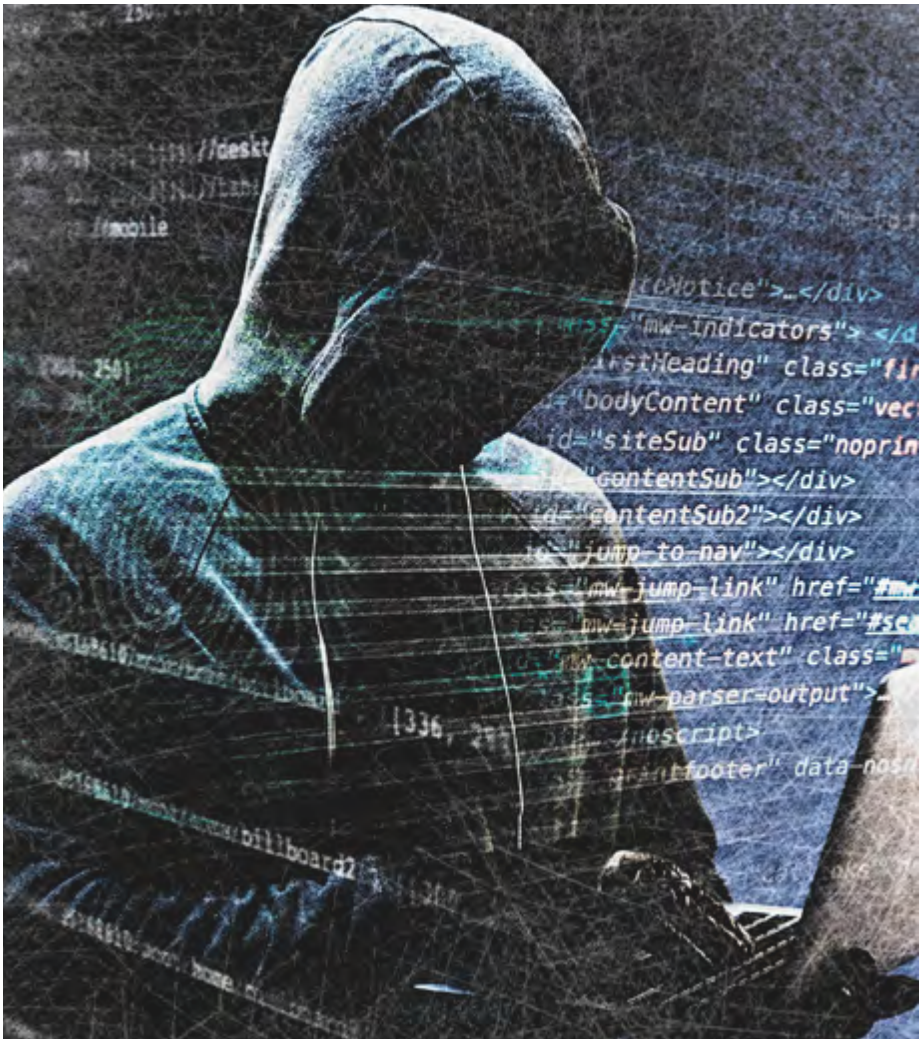
Russian DDoS[4] attacks still come in waves against Latvian government and municipal institutions and critical infrastructure. The goal of such

[2] ENISA Threat Landscape 2025. October 2025, p.2 https://ej.uz/enisa

[3] Russian cyber-criminal groups, who carry out ideologically or politically motivated cyber-attacks.

[4] Distributed Denial-of-Service attack (DDoS) – cyber-attacks intended to overwhelm web servers with requests,causing overload and rendering the website inaccessible.

attacks is to disrupt services and availability of information, spread doubt in society, and undermine trust in public institutions and vital services. DDoS attacks are frequently tied to nationally relevant dates or political decisions and announcements. For instance, in late July Russian hacktivists carried out a large DDoS attack after a Latvian company was announced as winners of an international drone procurement. In most cases DDoS attacks have little or no effect on services' availability. To minimize the impact of DDoS campaigns, organizations in Latvia are recommended to use services designed to defend against DDoS attacks. Latvian Ministry of Defence is funding a centralized DDoS defence service that is free of charge for public institutions. The provision of this service is delegated to Latvian State Radio and Television Centre (LVRTC)[5].



[5] https://www.lvrtc.lv/pakalpojumi/valsts_sektoram/ddos/

SUPERVISION OF ICT CRITICAL INFRASTRUCTURE

Information and communications technology (ICT) critical infrastructure (CI) includes ICT infrastructure, information systems, technical and information resources which are crucial for fulfilling vital societal functions, ensuring public health protection, security, economic, and social welfare. The destruction or disruption of ICT CI would significantly impact the implementation of state functions. Protection of ICT CI ensures the availability and continuity of the above-mentioned services and prevents threats to society and national security.

Since Russia's full-scale invasion of Ukraine in 2022, the threat to all CI, including ICT CI, has considerably increased. Changes and improvements to legislation governing ICT CI are an important prerequisite for effective supervision and protection of ICT CI.

On 1 September 2024, the National Cybersecurity Law came into force. The law applies to critical infrastructure of information and communication technology (ICT) as well as providers of essential and important services.

On 25 June 2025, the Cabinet of Ministers adopted Cabinet Regulation No. 397 "Minimum Cybersecurity Requirements" on the basis of the National Cybersecurity Law. The new regulation sets a number of requirements for entities that are subject to the National Cybersecurity Law.

As part of the supervision of ICT critical infrastructure, SAB:

- controls the compliance with cybersecurity requirements;
- verifies and approves applicants for the role of Cybersecurity Manager;
- performs security checks for natural and legal persons needing to access ICT critical infrastructure facilities;
- approves security classes of information systems and resources;
- performs on-site checks and remotely monitors information and communication technologies;
- verifies data and documents related to risk management and elimination of deficiencies detected in conformity evaluations and security scans of the entity's electronic communications networks and information systems;
- performs in-person and remote consultations regarding

implementation of the National Cybersecurity Law and Cabinet Regulation No. 397.

According to the requirements of the National Cybersecurity Law and related Cabinet Regulation No. 397, SAB has carried out verification and approval of the applicants for the role of Cybersecurity Manager and analysed self-assessment reports to determine whether the particular entity has complied with the requirements set out in legislation. According to the National Cybersecurity Law, all entities had to submit their self-assessment report and notification regarding the Cybersecurity Manager position by 1 October 2025.

As part of ICT CI supervision, in 2025 SAB has received 710 requests and has carried out security checks of 681 legal persons and 3956 natural persons.

PROTECTION OF CLASSIFIED INFORMATION

Latvian national classified information – the Official Secret – is information the loss or unlawful disclosure of which may harm the security, economic or political interests of the state.

According to the Law "On Official Secret", the status of Official Secret also applies to NATO, EU, and foreign classified information.

Security oversight of the protection of classified information is a set of measures that includes, e.g., security checks, vetting, and inspections of persons, companies, facilities, and information systems. It also comprises verification of procedures for the protection of information and circulation of documents, consultations on issues related to protection of classified information and any risks that must be taken into account when working with such information, as well as the development of legislation, including international agreements on the exchange and protection of classified information.

The ability to provide protection of NATO and EU classified information is a prerequisite for Latvia to be considered a full-fledged partner in these organizations, while the protection of foreign classified information is an essential condition for effective cooperation with each of our allies.

The security oversight of protection of national classified information is carried out by all three state security agencies – SAB, the State Security Service, and the Defence Intelligence and Security Service. SAB as the Latvian National Security Authority (NSA) is responsible for security oversight and protection of NATO and EU classified information in Latvia.

Regular assessment visits are conducted to check the compliance of the Latvian system for protection of NATO and EU classified information with NATO and EU security requirements.

Personnel security

Vetting for access to national classified information is carried out by all three state security agencies. Security clearances for access to SEVIŠĶI SLEPENI (Latvian national TOP SECRET) information are issued only by SAB, based on the vetting carried out by all three state security agencies. In 2025, SAB issued 1134 security clearances for the access to national classified information, including 348 security clearances for access to SEVIŠĶI SLEPENI information.

In 2025, SAB denied access to the national classified information in 3 cases. No previously issued security clearances were revoked. The decision of a state security agency to deny access to the national classified information can be contested to the Prosecutor General whose decision can be further appealed to the Regional Administrative Court. In 2025, 2 decisions taken by SAB to deny access to the national classified information were contested to the Prosecutor General. In one case, the Prosecutor General is still assessing the SAB's decision, while the other decision was further appealed to the Regional Administrative Court. The court upheld the SAB's decision.

Security clearances for access to NATO and EU classified information can only be issued to people who have already been granted access to the national classified information. NATO and EU clearances are issued only by SAB based on a vetting that includes analysis of the vetting materials for access to the national classified information and gathering of additional information necessary to make the final decision regarding granting access to NATO and EU classified information. In 2025, SAB issued 2170 security clearances for access to NATO classified information, and 2192 security clearances for access to EU classified information.

In 2025, SAB denied access to NATO and EU classified information in 2 cases. SAB's decision to deny access to classified information of foreign states and international organisations is final and cannot be further appealed.

SAB also conducts other security checks in cases where a person does not require access to classified information, but it is still important to assess potential security risks. These were mostly related to access to critical infrastructure mentioned in the previous chapter; however, in 77 cases, SAB performed security checks to provide opinions to government institutions in various other cases foreseen in the legislation (potential honorary consuls, etc.).

We would like to highlight the following as particularly high-risk criteria for people who were vetted for access to both the national and NATO and EU classified information in 2025:

- mental health disorders (including gambling, alcohol, drug, or psychotropic substance addiction);
- financial difficulties (excessive debts, including regular use of short-term loans, or unclear financial transactions);
- regular trips to risk countries, such as Russia, Belarus, and other CIS countries, China, or contacts with citizens of these countries;

- certain negative personality traits and provision of false information or concealment of information during the vetting process.

If, during the vetting, there is a reason to suspect that the person has mental and behavioural disorders that could affect their ability to comply with the requirements for protection of official secret, the person is requested to undergo a health examination in accordance with the Cabinet of Ministers Regulation No. 471 of 28 July 2020 "Regulation on Health Examination for Persons Applying for a Personnel Security Clearance for Access to Official Secret".

After evaluating the risk factors identified during the vetting, a decision can be made to grant access to classified information for a reduced period of validity or deny access to classified information.

Industrial security

Facility Security Clearance (FSC) confirms the right of a company to participate in public procurements involving access to the national, NATO and EU classified information as well as the ability of the company to protect such information.

The vetting of companies for access to the national classified information is carried out by all of the three state security agencies, whereas the vetting for access to NATO and EU classified information is carried out only by SAB. The decisions on issuing FSCs are only taken by SAB.

As of January 2026, there were 98 valid FSCs for access to the national classified information, 6 for access to NATO and 5 for access to EU classified information. In 2025, SAB has issued 32 FSCs.

The number of companies that need to be vetted for an FSC has grown significantly over the last three years due to the large increase of defence investments that came as a response to Russia's full-scale invasion of Ukraine. It is important to remember that FSC is only necessary for contracts that include access to or handling of classified information. Not all defence-related contracts have such provisions. We would like to remind all government institutions that the request for an FSC in a procurement has to be confirmed with the state security agency providing security oversight for the particular institution, and urge all companies to carefully examine whether they actually need access to classified information before submitting an application for an FSC.

In 2025 SAB had no cases of refusal to issue an FSC. There were 4 cases in which companies withdrew their applications and 13 other cases in which vetting was discontinued due to other reasons.

Most of the risks identified in 2025 were related to "key people"[6] of the company whose vetting led to findings that gave grounds to doubt the reliability of the person. These included personality traits and behaviour as well as family ties that indicated high risks of influence (e.g., threats of blackmail or bribery). In several cases, company representatives tried to provide SAB with false information about themselves or persons who actually control the company and benefit from its activities.

Physical security and security of information

The inspection and certification of premises of government institutions and companies used for handling of the national classified information is done by all of the three state security agencies, while the premises for handling of NATO and EU classified information are only certified by SAB. The certification process includes inspection of the physical, procedural, and personnel security as well as management of classified information.

The Central Registry of SAB supervises and controls the circulation and protection of all NATO and EU classified information.

In 2025, SAB carried out inspections and certified government premises in 16 institutions and 13 companies.

During inspections and consultations, we observed that government institutions show a lack of understanding of the requirements of Cabinet of Ministers Regulation No. 822 of 19 December 2023 "Regulation on the Protection of Official Secret, Classified Information of the North Atlantic Treaty Organization, the European Union and Foreign Institutions", and a low initiative to implement and comply with the regulations.

Accreditation of classified information systems and information security in electronic environment

In accordance with the provisions of Article 7, Paragraph 7 of the Law On Official Secret, SAB inspects and accredits information systems in which classified information is processed, develops security requirements for the protection of classified information in electronic environment, and determines encryption systems for protection of classified information, as well as performs the registration and administration of encryption equipment and materials.

In 2025, SAB accredited 122 classified information systems.

[6] In order for a company to be granted an FSC, its participants (natural persons), members of the board and council, authorized signatories, beneficiaries, and facility security officers must meet the criteria set out in legislation for access to classified information.

International cooperation

SAB negotiates and drafts bilateral agreements on the exchange and protection of classified information (security agreements). When developing these agreements, SAB takes into account the areas where a regulatory framework for exchange of classified information is currently needed, such as the presence of NATO forces in Latvia or cooperation with a country in the field of industrial security. Negotiating agreements is a long-term process involving two countries with different regulatory frameworks, both in terms of the protection of classified information and the procedures for drafting and ratifying agreements.

In 2025, SAB worked on security agreements with Switzerland, Ukraine, Poland, and North Macedonia. It is planned to start the negotiation process for amendments to the security agreement with the Czech Republic, and new security agreements with Sweden, Belgium, Singapore, and the Organisation for Joint Armament Cooperation (OCCAR).

As Latvian NSA, SAB takes part in NATO and EU forums where member states develop a unified framework for protection of classified information: NATO Security Committee, the Security Committee of the Council of European Union, the Security Expert Group of the European Commission, and the Security Committee of the European External Action Service.

SAB also represents Latvia in the Multinational Industrial Security Working Group (MISWG) which develops common principles and procedures for international cooperation in the field of defence and industrial security. Most of the procedures and documents developed by MISWG are also used by NATO and EU.

LEGAL MOBILE INTERCEPTION

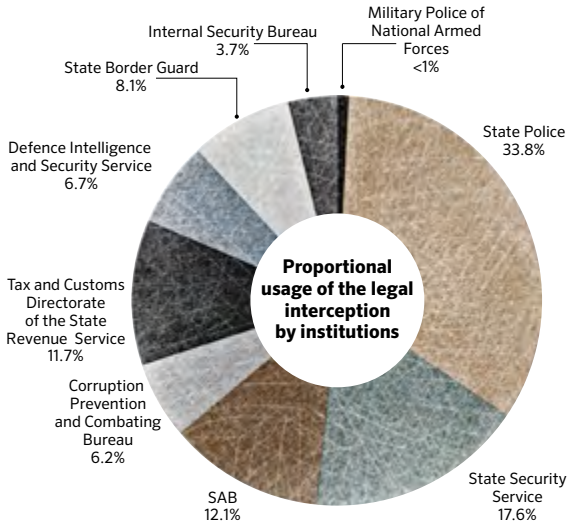
SAB hosts the technical facilities and equipment that provides legal mobile interception for law enforcement agencies and state security agencies. The data obtained during an interception are transferred to the initiator of the particular interception who has received a warrant from the Justice of the Supreme Court. The competence and responsibility of SAB include legal interception, protection of technical parameters and methodology of the interception as well as the protection of the obtained data from an unauthorized disclosure before the data are delivered to the initiator of the interception.

Prior to the beginning of a legal interception, SAB receives the necessary documentation from the initiator of the interception stating the following:

- lRegistration number of the initiating decision;
- Official who has taken the decision;
- Head of the institution who has confirmed the decision;
- Justice of the Supreme Court who has issued the warrant;
- Telephone number to be intercepted;
- Duration of the interception.

The legal supervision of mobile interception is provided by the Prosecutor General and specially authorized prosecutors. Parliamentary control is exercised through the National Security Committee of the Parliament.

As in previous years, SAB has not committed any violations regarding mobile interception in 2025. The proportional usage of the legal interception by law enforcement agencies and state security agencies is provided in the following chart.



CONTACT US

CONSTITUTION PROTECTION BUREAU (SAB)

Straumes iela 1, Riga, LV-1013, Latvia

www.sab.gov.lv

Phone: +371 67025407

E-mail: pasts@sab.gov.lv

X: @SAB_LV

FOR PRESS-RELATED INQUIRIES

Phone: +371 28386600

E-mail: prese@sab.gov.lv