ANNUAL PUBLIC REPORT 2017

The Constitution Protection Bureau (SAB) is one of three state security institutions of the Republic of Latvia. SAB is responsible for foreign intelligence, counter-intelligence and safeguarding of national, EU and NATO classified information.

Executive Summary

- Russia's foreign and security policies towards the West, including Latvia, are confrontational. More and more often Russia using various tools tries to influence domestic politics of EU and NATO member states. This includes interference in elections and attempts to manipulate public opinion. SAB's main task is to analyse and monitor Russia's activities and to carry out measures for strengthening national security.
- Throughout 2017 SAB continued to conduct counter-intelligence measures against several foreign intelligence and security services. The major threat against the interests of Latvia is caused by the activities of Russian intelligence and security services. The activities of Russian intelligence services in Latvia are carried out by using diplomatic cover or acting from Russia's territory. Latvia's security policy, defence capabilities and military sector remain one of the main priorities for Russian intelligence. There is an increased interest towards Latvian election processes.
- Western societies, including that of Latvia, are improving their ability to detect and critically assess Russian propaganda and influence activities by pro-Russian organizations under Kremlin's guidance. Kremlin is developing capabilities to conduct complex influence operations and cyber is a crucial part for such operations. For example, fake news are increasingly distributed by the use of cyber attacks.
- The number of cyber attacks conducted by foreign intelligence and security services against Latvia have increased almost twofold in the last 3-4 years. There are more than dozens of such cyber attacks in a year. Cyber espionage is mostly directed against governmental institutions, including branches of foreign policy, defence and home affairs.
- Distributed denial-of-service (DDoS) attacks have become a relatively widespread type of cyber attack that is aimed against information technology (IT) systems of various institutions. IT systems that ensure relevant state and public functions have to apply special cyber defence solutions. Such IT systems can face more than several hundreds of DDoS attack a year. According to SAB estimates, foreign intelligence services might be responsible for approximately 5 % of DDoS attacks.
- Russia invests significant resources in development of communications interception capabilities. Russian intelligence services are able to eavesdrop and control data flow if one of users is located in Russia or if both users are located outside of Russia, but data flow is routed through Russian communications infrastructure.
- Russia's influence activities in the Baltic region are carried out by pseudo-academic and experts' organizations that are established and controlled by Russia. More and more often Kaliningrad is used as a centre for such organizations, for example, "Rossiyskaya asociaciya Pribaltiyskih issledovaniy" and "Kaliningradskiy blogpost".

INTRODUCTION

The most important threat to Latvia's security is caused by Russia's aggressive foreign policy, aimed not only against Latvia, but also towards Baltic Sea region, EU and NATO. Increasing security risks also stem from Russia's military activities, however, significant threats are related to Russia's non-military influence tools that mostly are discreet, but with long-term effect. Russia's cyber capabilities and readiness to use them are one of the fastest growing security threats directed against the West. In recent years Russia has conducted several complex and notable operations in order to influence domestic political processes of the Western countries. Cyber and information space is widely used in such operations. It is highly likely that Russia poisoned the former Russian spy Sergey Skripal with a highly toxic substance in the United Kingdom on 04 March 2018. Incident highlights Russia's readiness to carry out increasingly aggressive operations in order to reach its goals. Russia is ready to continue with its confrontational policies.

In 2017 Russia's activities against Latvia consisted of Russia's influence activities in information space, work with influence agents, including compatriots' policy, use of influence tools, as well as activities of Russian intelligence services and increasing cyber activity.

RUSSIA

In 2017 Russia continued its confrontational foreign and security policy towards the West regarding its actions, but also political rhetoric and propaganda. It is a result of Russian elite's belief that the West can influence, support and finance protests and public dissatisfaction that could threaten stability of Russian regime. Russian elite also perceives NATO and EU's integration and enlargement as an increased threat. Russia fears that it could decrease Russia's geopolitical role and expand the space of the Western values, therefore possibly changing Russia's social environment in long-term.

Due to these positions, Russia actively tried to extend its geopolitical influence in 2017, for example, by increasing Russian involvement in crisis regions like Afghanistan, Libya, North Korea and Syria. In several cases Russia's main motive was restriction of US influence. On North Korean issue Russia's involvement was limited to diplomatic tools in UN Security Council, while in Syrian conflict Russia used a broad spectrum of tactical tools, including military force, and allowed Assad to use chemical weapons. Russia's policy in Syria clearly signals that regime change in Syria is impossible without Kremlin's approval.

In 2017 Russia continued its attempts to destabilize Transatlantic relations within NATO, weaken EU's unity and reduce the significance of EU common foreign policy. In order to neutralize EU and NATO influence, Russia continues its aggressive foreign policy towards Balkan countries (Montenegro, Bosnia and Herzegovina), Moldova, Ukraine and Georgia. Russia uses cyber attacks, propaganda and disinformation campaigns, intelligence services and other hybrid tactics to achieve its goals. However, Russia has not succeeded and there are positive developments in the foreign policies of these countries.

There is a new trend within Russia's foreign and security policies in 2017. Using various tools Russia tries to influence domestic politics of EU and NATO member states in its favour. Investigation on Russia's attempts to influence the result of US presidential election in 2016 continues. In similar way Russia was involved in French and German elections. Russia also tried to influence domestic situation in Spain.

Russia tries to influence internal processes of EU and NATO member states by the use of political-diplomatic tools, economic relations (especially energy), demonstration of military potential, cyber capabilities, as well as by purposefully spreading disinformation and propaganda. Russia's interests and leverage towards different countries vary due to several factors – history,

relations with local elites, cultural ties, influence possibilities etc. Russia's security structures, including Ministry of Defence and intelligence services, have an increasing role in formation of Russia's foreign and security policies.

Russia's policy in Baltic Sea region stems from Russia's adversarial stance towards the US and Transatlantic relations. The strategic objective of military exercise ZAPAD-2017 was aimed against NATO, especially US military presence in Baltic states and Poland.

In overall Russian interests are changeable and are adjusted for particular situations. In 2017 a large focus of Russia's foreign and internal politics was drawn towards downplaying the Russian athletes' doping scandal. In this matter Russia tried to influence international organizations, distribute Kremlin's propaganda and disinformation by creating anti-Western narratives that were favourable to Russia. Russia widely used hybrid tactics in these activities.

Throughout 2017 Russia in several formats has pushed for cancellation, mitigation or at least review of the Western sanctions, which were implemented after Russia's aggression against Ukraine. Issue of sanctions is one of the priorities of Russia's foreign policy, but at the same time it is used for internal needs as well in order to justify Russia's policies towards the West.

Russia's foreign policy is closely linked with its ruling elite's interest to guarantee the regime's stability. 2017 was a particularly significant year as various governmental levels prepared for presidential elections. Regional elections in 2017 indicated a very low public interest about politics, apathy and indifference towards Kremlin's propaganda. Regional elections had a low turnout, especially in Moscow and Saint Petersburg. Kremlin's political activities in 2017 were aimed to increase the turnout in presidential elections as much as possible, otherwise Russia's president Vladimir Putin's legitimacy could be questioned.

Russia's internal developments indicate ruling elite's attempts to create a new ideological platform that could unite Russian society and various ethnicities. "Eurasian project" is developed as a framework where Russian chauvinistic, socialist, Orthodox and militarism ideas would be combined in Kremlin's media space. With such a project Russian elite tries to overcome the split society by creating synthesis of leftist and even monarchic ideas that are based on Russian imperial and USSR historical experience. Right-wing and liberal societal groups are purposefully marginalized and oppressed as they are perceived as inadequate for current Russia's relations with the West.

Russia's economic and social problems worsened Russia's internal situation in 2017. Although Russia's macro-economic indicators indicate that economic recession ended in 2017, economic growth is low and does not meet Kremlin's political requirements. Real income of Russians continued to decrease in 2017, especially in regions. Deterioration of living standard is imperilling Kremlin's informal social contract that for years has allowed to increase the income for Russians, at the same time restricting political and civic freedoms. Although oil price is currently favourable for Russia, the government finds it difficult to fulfil its budgetary commitments as Russia has spent its reserve funds. Economic situation is worsened by international sanctions, financial problems in Russian bank system, avoidance of economic and social reforms (for example, in tax and pension systems), insufficient amount of foreign and internal investments, domination of state-owned large corporations and inefficient work of Russian institutions. Such social and economic situation aggravated infighting among Russian elite's groups for resources and official positions.

RUSSIAN INTELLIGENCE AND SECURITY SERVICES

Activities conducted by non-NATO and non-EU foreign intelligence and security services constitute a major security threat not only against Latvian, but also against EU, NATO and

collective security interests. The main objective of the activities of the mentioned services is to gain publicly inaccessible and pre-emptive information which provides foreign government with advantages for decision making on economic, political and military issues. Besides information collection intelligence and security services implement active measures with the aim to influence decision making process of Latvian, EU and NATO institutions as well as public opinion.

Throughout 2017 SAB continued to conduct counter-intelligence measures against several foreign intelligence and security services. The major threat against the interests of Latvia is caused by the activities of Russian intelligence and security services. Activities of hostile intelligence and security services from other countries are assessed as moderate and not posing a significant threat to Latvian interests. In order to collect intelligence and conduct active measures, intelligence services use versatile working methods – information sources and contact-persons, information collection from open sources, as well as different technical capabilities within cyber space and signal intelligence field.

Russian intelligence services carry out deliberate and systematic work in order to obtain intelligence about most significant aspects of Latvia's internal, foreign, security, economic and energy policies. Russian services also follow social processes and public attitudes within Latvia. Latvia's security policy, defence capabilities and military sector still are one of the main priorities for Russian intelligence. Detailed attention is paid to Latvia's participation in NATO, especially NATO actions and strategy in the region. Russian intelligence services are also interested in the work of Latvian law enforcement and security institutions, including personnel, finances, cooperation, subordination and action plans for crisis situations. Also in 2017 Russian intelligence services were increasingly interested in border security issues.

In regard to Latvian domestic politics, Russian intelligence services are interested in a broad spectrum of issues, especially in all major political events and their "behind-the-scenes". There is a high intelligence interest in regard to election processes, positions of political parties, political leaders and main officials. Also political and social processes in municipalities, including in border area, are of an interest to Russian intelligence services. In 2017 Russian services followed the municipal elections, analysed the possible outcome, as well as assessed how election result will influence the positions of political parties for upcoming Latvian parliamentary elections in autumn 2018.

Russian intelligence services conduct activities against Latvia from different positions, for example, by using legal residencies with diplomatic cover. During last few years possibilities for Russian intelligence services to use diplomatic cover for intelligence collection is encumbered as the official cooperation in several fields between Latvia and Russia has diminished. Society's attention against suspicious "diplomatic" activity has also increased.

Russian intelligence services are particularly active in Latvia's border area. Federal Security Service (FSB) controls Russia's border zone and border by using Russia's Border Service. For operational work FSB often use other institutions that have to conduct legitimate functions on border, for example, Federal Customs Service or Main Directorate for Migration Affairs.

Foreign intelligence services, including those of Russia, work against Latvia's citizens not only from their territories, but also from third countries and international organizations. It is widely common in Russia that intelligence services use the cover of other institutions and organizations, usually taking positions that are related to international cooperation. Intelligence services use the cover of Russian government institutions, municipalities, non-governmental organizations, media and universities.

Russian intelligence services also conduct activities against Latvia in information and cyber space, which have cross-border nature. Services have special units that plan and carry out cyber attacks, information and psychological operations. Russian intelligence services also have necessary

infrastructure for such activities in information space – they have access to Kremlin's media and maintain their own resources in internet.

RUSSIAN INFLUENCE ACTIVITIES AND PROPAGANDA

Russia invests significant resources in its informational influence and propaganda activities in the West. The most notable propaganda projects in English are TV channel "RT" and multimedia platform "Sputnik". Russia has allocated financial resources for maintaining and expanding these projects. But in general the influence of Kremlin's propaganda media in the West is limited and their contribution to advancing issues, relevant to Russia, is insignificant.

In parallel to traditional propaganda methods, in 2016-2017 Kremlin conducted several complex influence operations, related to elections in USA, France and Germany with an aim to influence the election result. Russia used combination of several methods in these operations, while hiding its participation. For example, as a result of cyber espionage, Russia acquired content of politicians' e-mails and documents, which were selectively published in media and internet. Information campaigns followed, for example, the published materials were commented by various experts, other media outlets republished the information, there were organized "trolling" campaigns and activities in social networks. Some parts of these activities were robotised in order to gain massive result. Genuine information was combined with fake news. It is possible that Kremlin might use similar model of influence operations in the future. However, with each case the Western attention and abilities to resist influence operations increase. It might force Kremlin to review its methods and look for different tactics of influence operations.

Russia's influence activities and propaganda tasks in Latvia correspond to Russia's foreign policy objectives to increase its role in the region, while weakening NATO and EU, as well as Baltic states' positions in these organizations. Influence activities are aimed towards weakening of Latvia's statehood by promoting society's distrust towards government, questioning Latvia's geopolitical direction in NATO and EU, discrediting Latvia at international level, cultivating conflict potential, emphasizing differences of ethnic, linguistic issues and interpretation of history. Information space is crucial for promoting "Russkiy Mir" and Kremlin world-view. The main topics for Russian informational activities have not changed in recent years. Depending on situation, Russia changes emphasis and adjusts messages. In 2017 one of the main topics for Russian influence activities was NATO enhanced Forward Presence (eFP). Russia spread misleading messages that NATO destabilizes regional security situation, eFP is against Latvia's interests and poses threats to civilians.

The main foundation for Russian informational influence in Latvia is laid by retranslated TV channels, controlled by Kremlin. "Rossiya Sedognya" structures "Sputniknews" and "Baltnews" continue their work in Baltic states, but their influence is limited. Russian influence activities in Baltic region are also carried out by Russian established and controlled pseudo-academic and expert organizations. The most visible examples in 2017 were foundation "Istoricheskaya pamyat", "Rossiyskaya asociaciya Pribaltiyskih issledovaniy" and discussion club "Kaliningradskiy blogpost". The last two were founded in and are working from Kaliningrad, which more and more often is seen as a centre for conducting influence activities against Baltic states. Kaliningrad is used due to its geographical location and options, provided by Immanuel Kant Baltic Federal University. Several projects, coordinated or initiated by Russia's Presidential Administration's Directorate for Interregional Relations and Cultural Contacts with Foreign Countries, work from Kaliningrad: web portal RuBaltic.ru, centre "Russkaya Baltika", regional desk of information agency REGNUM etc.

"Kalinigradskiy blogpost" organizes monthly one-sided discussions, where experts bring up issues relevant to Russia. Particular emphasis is placed on distributing conclusions of such

discussions on internet and social networks. Discussions are devoted to topics like NATO and Baltic states' threats towards to Kaliningrad, Russophobia and Euroscepticism in Baltic states, etc.

"Rossiyskaya asociaciya Pribaltiyskih issledovaniy" unites individual influence agents and is presented as interdisciplinary professional association for researching Baltic history and current developments, as well as for consolidation of such experts in Russia. In reality there are only few activities of several persons and their partners, who try to imitate academic work. Although their conferences are announced as international ones, events are mostly attended by the organizers themselves. The status of such conferences is artificially increased by exaggerated publicity. "Rossiyskaya asociaciya Pribaltiyskih issledovaniy" publishes pseudo-scientific materials, including on so-called discrimination of Russian compatriots in Baltic states. In 2017 this organization published book "Citizens and non-citizens: Political-legal division of Latvian inhabitants in post-Soviet era" by V. Buzajevs.

One of the most active organizer of informational activities against Latvia and Baltic states is Vladimir Simindey, who participates both in "Rossiyskaya asociaciya Pribaltiyskih issledovaniy" and foundation "Istoricheskaya pamyat". Although V. Simindey lacks any real academic work and publications, he positions himself as an expert on Baltic history and current developments, as well as defender against history falsification in Baltic states. In 2017 V. Simindey had access to a large amount of publicly unavailable and specifically selected documents from FSB Central archive and other closed archives for creating propaganda materials.

These and other declassified documents were used for information activities against Baltic states. Documents are deliberately selected, their main topic is the contribution of USSR, Soviet nation and Red Army in defeating Nazism that ensured the victory of anti-Hitler coalition in World War II, as well as fight against Nazis and struggle against heroization of those who opposed the Soviet Union. Attention is also paid to economic history of Baltic states after World War II, demonstrating how Soviet Union's central government helped to develop them.

In general Latvian and Baltic societies view Russian propaganda more and more critically. The ability to recognize Russian propaganda channels and messages has increased. Thus Russia carries out more specific influence operations by combining different methods in order to distribute provocative and discrediting information in Baltic states. In 2017 there were several cases when cyber capabilities were used for placing misleading news in internet. As one of the main priorities for Russian intelligence services in the region is NATO eFP, internet media were infiltrated with news that discredit eFP or portray it as a threat to society. Notable example is a cyber attack in April 2017, when fake information was placed in news feed of Lithuanian and Russian editions of Lithuanian news agency BNS, for example, that US soldiers in Latvia have been poisoned with pepper gas, a large amounts of the gas is dumped in Baltic Sea and that only Kremlin knows when the ecological bomb will explode. Cyber attack was used in order to post such falsified information.

Another example is from June 2017, when it was posted on website reddit.com that an American bomber B-52 has crashed in Lithuania and therefore destroyed a house. In order to create credibility, the author had republished several genuine news beforehand from other sources. Information about crash was posted in such way that it created an impression of being republished from website of US Department of Defence. The information was then republished by several media and websites, for example, on pro-Russian portal www.baltijalv.lv, where it was illustrated with video from "crash site". The information on this portal was published by hacking its server and copying the post on news page without using the official procedure of posting.

CYBERTHREATS

The largest cyber threat to Latvia is posed by non-NATO and non-EU intelligence services, cyber units of armed forces, as well as state sponsored hacktivists. Cyberspace is also used by

terrorist organizations which mostly distribute propaganda and recruit fighters. Threats are also posed by cyber criminals and cyber hooligans. The main goal of cyber criminals is profiting, however, through their activity they might paralyse significant information technology (IT) systems or acquire sensitive date. The activity of cyber hooligans is increasing, they mostly try to check the vulnerability of different IT systems.

The main cyber threat to Latvia is posed by Russia. Russia's cyber capabilities and readiness to use them are increasing. Currently it is considered one of the most rapidly growing security threats to the West, including Latvia. Cyber activities are now a regular part of Russian policies, occurring in almost all Russia's foreign and military activities. In recent years Russia has conducted espionage campaigns against the Western institutions. Russia has also used cyber capabilities in order to carry out significant information operations with an aim to demonstrate its power and influence domestic politics of other countries.

Russia invests significant resources for development of communications interception capabilities. Russian intelligence services are able to eavesdrop and control data flow if one of users is located in Russia, as well as in cases when both users are located outside of Russia, but data flow is routed through Russian communications infrastructure. Such capabilities are fully guaranteed by FSB controlled system for operative investigative activities SORM. Russian intelligence services also develop capabilities to access mobile devices with internet connection.

In 2017 SAB identified several cyberattacks carried out by foreign intelligence services or their led hacker groups which mostly targeted state institutions. The number of such cyber attacks have increased almost twofold in last 3-4 years. There are more than dozens of such cyber attacks in a year. Most of cyberattacks in Latvia are carried out for espionage purposes by the use of spear-phishing method. Victim receives a false email which entices the receiver to open it. Once opened, it infects the receiver's computer. The content of the spear-phishing email frequently is designed for the specific interests of the victim.

In recent months Latvian society's attention has been brought to the issue of IT system security of different governmental and non-govermental institutions against distributed denial-of-service (DDoS) attacks. Such attacks have become one of the most widespread cyber attacks. IT systems of institutions, that fulfil relevant state and public functions, are listed as IT critical infrastructure. The list is systematically and regularly reviewed. These institutions have to implement specific security requirements that also increase resistance against cyber attacks. If technically possible, cyber defence solutions against DDoS attacks are implemented in such IT systems, and so far this protection has proved itself to be successful. Specially protected IT systems might face up to several hundreds of DDoS attacks per year. It is extremely difficult to identify the real initiators responsible for DDoS attacks. According to SAB estimates, foreign intelligence services might be responsible for up to 5 % of all DDoS attacks that are targeted against specially protected IT systems.

Although cyber threats to Latvia are relatively high, there are some positive trends in regard to strengthening cyber security. In recent years Latvian security services have increased their ability to detect cyber attacks by foreign intelligence services, measures for securing IT systems are being implemented, society's understanding about cyber security is increasing, including readiness of governmental organizations to invest in developing IT security. CERT.LV, the information technology security incident response institution of Latvia, is significantly contributing to cyber security. Large role is attributed to collective security measures, including cooperation between Latvian security services and foreign partners. Taking into account the risk of possible increase of Russian cyber activities in regard to Latvian parliamentary elections in autumn 2018, in 2017 SAB monitored any possible indications concerning usage of cyber attacks to influence the elections. SAB will continue this work in 2018.

PROTECTION OF NATO AND EU CLASSIFIED INFORMATION

SAB as the National Security Authority (NSA) is responsible for the protection of NATO and EU classified information which is an essential security aspect for NATO and EU, and ability to provide it is a cornerstone for the Republic of Latvia to be considered as a full member of both organizations. Protection of classified information is a system of different security aspects which includes personnel security, physical security, document management security, industrial security and information assurance. SAB as the NSA is responsible for supervision and accreditation of all government entities and bodies that require access to NATO and EU classified information. Regular NATO and EU inspections are conducted in the Republic of Latvia to ensure that all international obligations and standards are met.

In 2017 SAB carried out the vetting procedures and issued 1799 NATO and 1860 EU certificates of personnel security clearances. In 4 cases access to NATO and EU classified information were denied.

PROTECTION OF NATIONAL CLASSIFIED INFORMATION

In accordance with the “Law on State Secrets”, SAB in conjunction with the Security Police and the Defence Intelligence and Security Service is responsible for safeguarding national classified information. As part of classified information protection measures SAB conducts the vetting procedures of candidates requiring access to classified information, certifies premises where classified information is stored and ensures accreditation of information and communication systems that are used to produce and transfer classified information.

In 2017 SAB prepared for issuing 584 national security clearances and denied access to classified information in 23 cases, including the appealing procedures for the cases that have been submitted to SAB based on the decisions by the Security Police and the Defence Intelligence and Security Service. According to existing procedures, SAB also serves as an appeals institution in the case of taking negative decisions of the other two state security institutions (Security police and Defence Intelligence and Security Service) regarding the refusal procedure to grant the national security clearances. The relevant criteria that all candidates must meet in order to gain access to classified information are stipulated in the “Law on State Secrets” paragraph 9.

Negative decision taken by the Director of SAB regarding access to classified information can be appealed to the Prosecutor General of the Republic of Latvia. In 2017 the Prosecutor General's office received 17 such appeal cases. The Prosecutor General judged that in 16 cases decisions by SAB were justified and in accordance with the existing law. In one case the Prosecutor General has partially and temporarily repealed the decision, passing it for reconsideration.

INDUSTRIAL SECURITY

The Facility security clearance (FSC) confirms the rights for all private entities (companies) wishing to provide services or goods to state institutions where access to national, NATO and EU classified information is required. The FSC and procedures that are taken to receive it ensures that private entities have the necessary measures in place to safeguard classified information. According to the procedures the necessary inspections can be conducted by any of the three state security institutions, which submit their results to SAB for the final decision to issue/deny FSC.

There are 122 Facility security clearances issued by SAB valid for the work with National classified information and 4 FSC valid for the work with NATO classified information as of the beginning 2018. During the same period of time SAB has decided to deny FSC to 6 entities, and in

5 cases FSC abolished. All negative decisions taken by SAB can be appealed to the Prosecutor General whose decision then is final. There were 4 appeals in 2017 and in all cases SAB decision remained unchanged.

It is necessary to undergo personnel vetting procedures for the entities in order to obtain FSC. During 2017 SAB has issued 243 National Personnel Security Clearances which allows to work with national classified information, 13 NATO Personnel Security Clearances for work with NATO classified information, and 10 National Personnel Security Clearances were denied.

LEGAL MOBILE INTERCEPTION

SAB hosts the technical facilities and equipment that ensures legal mobile interception for all law enforcement, security and intelligence agencies. The legal basis for all operation activities including interception is the Investigatory Operations Law. Legal interception can be conducted only on the request of the relevant agency having obtained a warrant from the Justice of the Supreme Court. SAB ensures the data collection, security and safety of the obtained data and its transfer to the relevant body conducting the operational activity.

Before to begin the process of legal mobile interception SAB receives the part of decision of operational activity where the following is stated:

- registration number of the decision,
- official who has taken the decision,
- head of service who has confirmed the decision,
- Judge of the Supreme Court who issued the warranty,
- telephone number which is under control,
- deadline when control over telephone ends.

The legal supervision of mobile interception and all other operational activities according to Latvian legislation is ensured by the Prosecutor General's office. Parliamentary control is exercised through the National Security Committee of Saeima (Parliament). In 2017 as in previous years all legal interceptions were conducted in accordance with the law. The proportional usage of the legal interception system by law enforcement agencies, security and intelligence services is provided in the following table:

State Police	40,4%
Security Police	19,9%
Constitution Protection Bureau	12,2%
State Border Guard	10,1%
Defence Intelligence and Security Service	8,7%
Customs Police of the State Revenue Service	3,3%
Financial Police of the State Revenue Service	3,3%
The Corruption Prevention and Combating Bureau	2,1%