Annual Report of the Security Information Service for 2017

Table of Contents:

1. The Nature and Scope of Intelligence Activities 2

2. Intelligence Activities and Findings 3

2.1. Protection of Major Economic Interests 4

2.2. Counterintelligence Activities 6

2.3. Protection of the Constitutionality and of the Democratic Foundations of the Czech Republic ..9

2.4. Terrorism 13

2.5. Proliferation of Weapons of Mass Destruction 14

2.6. Cybersecurity 15

3. Protection of Classified Information 18

3.1. Administrative Security 18

3.2. Security of Information and Communication Systems 18

3.3. Physical Security 18

3.4. Crisis Management 18

4. Cooperation with Intelligence Services of the Czech Republic and with other State Authorities 19

4.1. Cooperation with Intelligence Services of the Czech Republic 19

4.2. Cooperation with the Police of the Czech Republic 19

4.3. Cooperation with other State Authorities and Institutions 20

5. Cooperation with Intelligence Services of Foreign Powers 22

6. Oversight 23

6.1. External Oversight 24

6.2. Internal Audit 24

7. Maintenance of Discipline; Handling Requests and Complaints 26

7.1. Investigation of Conduct Suspected of Having the Traits of a Misdemeanor, of a Disciplinary Infraction, and of other Infractions 26

7.2. Investigations of Complaints and Notifications 26

8. Budget. 27

1. The Nature and Scope of Intelligence Activities

The activities, the status and the scope of powers and responsibilities of the Security Information Service (BIS) as an intelligence service of a democratic state are provided for in relevant legislation, especially in Act No. 153/1994, on the Intelligence Services of the Czech Republic, as amended, and in Act No. 154/1994, on the Security Information Service, as amended. The BIS is also governed in its activities by the Constitution of the Czech Republic, the Charter of Fundamental Rights and Freedoms, international treaties, and other legal regulations of the Czech Republic.

Under Section 2 of Act No. 153/1994, intelligence services are state agencies for the acquisition, collection and evaluation of information (hereinafter referred to as "securing information") important for protecting the constitutional order, major economic interests, and the security and defense of the Czech Republic. Under Section 3 of Act No. 153/1994, the BIS is an intelligence service securing information within its powers and responsibilities defined in Section 5, Paragraph 1 of Act No. 153/1994 on:

- schemes and activities directed against the democratic foundations, the sovereignty, and territorial integrity of the Czech Republic,
- the intelligence services of foreign powers,
- activities endangering state and official secrets,
- activities, the consequences of which may jeopardize the security or major economic interests of the Czech Republic,
- organized crime and terrorism.

Under Section 5, Paragraph 4 of Act No. 153/1994, the BIS also fulfills further tasks as defined by specific legislation (e.g. Act No. 412/2005, on the Protection of Classified Information and Security Clearance, as amended) or international treaties, by which the Czech Republic is bound.

Furthermore, Section 7 of Act No. 153/1994 stipulates that the responsibility for the activities of the BIS and for the coordination of its operation lies with the Government. According to Section 8, Paragraph 4 of this Act, the Government assigns tasks to the BIS within the scope of the Service's powers and responsibilities. The President of the Czech Republic is entitled to task the BIS with the knowledge of the Government and within its powers and responsibilities.

To fulfill its tasks, the BIS is authorized to cooperate with other intelligence services of the Czech Republic. Section 9 of Act No. 153/1994 stipulates that this cooperation must be based on agreements concluded between the intelligence services with the consent of the Government.

Under Section 10 of Act No. 153/1994, the BIS may cooperate with intelligence services of foreign powers only with the consent of the Government.

2. Intelligence Activities and Findings

A summary of all the intelligence activities, in which the BIS engaged in 2017, is part of the classified *Report on the Activities of the Security Information Service for 2017* – a report the BIS submits annually to the President of the Czech Republic and to the Government in accordance with Section 8, Paragraph 1 of Act No. 153/1994.

During the course of the year, again in accordance with Section 8 of Act No. 153/1994, the BIS informed entitled addressees about individual intelligence findings and the results of analyses, on which the overview of its activities in this public annual report is based. In 2017, the BIS submitted almost 500 documents to the President and Cabinet members. Further almost 1 000 documents were sent to relevant state authorities, the Police of the Czech Republic (in Czech: *Policie České republiky – PČR),* the Office for Foreign Relations and Information (in Czech: *Úřad pro zahraniční styky a informace – ÚZSI)*, and to Military Intelligence (in Czech: *Vojenské zpravodajství – VZ*).

Fulfilling its obligations under Act No. 412/2005, the BIS was asked by the National Security Authority (in Czech: *Národní bezpečnostní úřad – NBÚ*) to conduct more than 20 000 security clearance investigations for the issuance of security clearance certificates for natural and legal persons.

The BIS cooperates also with other state bodies (e.g. the Department for Asylum and Migration at the Ministry of the Interior, the Ministry of Foreign Affairs, the Ministry of Industry and Trade Licensing Administration) in areas falling under the remit of these authorities, e.g. residence permits in the Czech Republic, the MEDEVAC project, the arrangement of employment, international protection stipulated by the Asylum Act, or foreign trade in military equipment. The BIS received and processed requests concerning almost 100 000 natural and more than 1 000 legal persons.

In 2015, an amendment of Act No. 49/1997, on Civil Aviation, came into force, which stipulates provisions regarding reliability certificates issued to natural persons by the Civil Aviation Authority (in Czech: *Úřad pro civilní letectví - UCL)*. These screenings include a credibility assessment of natural persons conducted by the Czech Police. In relation to this matter, the BIS processed requests concerning more than 7 000 individuals.

In compliance with Article 9 of the Convention implementing the Schengen Agreement, the BIS, as the responsible Czech intelligence service, submits opinions on Schengen visa applications. In 2017, the BIS screened more than 1 700 000 applications.

2.1. Protection of Major Economic Interests

The composition of phenomena monitored by the BIS was similar to previous years. Their specific manifestations also concerned the same groups of entities – state-controlled business corporations, public-law entities, and regulatory institutions.

Serious state failures from a relatively distant past remained a source of acute problems. These failures kept generating situations that were difficult to deal with when the state was forced to choose only from bad solutions due to past mistakes. These negative consequences were often difficult to predict and even occurred at times when the primary issue might have seemed solved already. Ongoing efforts of private entities to illegitimately influence regulatory and control authorities, the decisions of which have a far-reaching and long-term effect on whole sectors, constituted an enduring trend that was significant for state economic interests.

In 2017, the BIS continued the trend of 2016 and informed law-enforcement authorities of suspected offences in an increased manner compared to previous years.

The state has a demand for a whole range of large-scale services and usually needs their long-term discharge. The state is also forced to organize for the service a new invitation for tender after certain time in order to adapt conditions to the current market situation and in an ideal case set them better. However, this aim is not always achieved when organizing the new invitation for tender. As the procuring entity, the state is often in a disadvantageous position that makes it in effect impossible to choose a new contractor. That simultaneously significantly limits state's ability to negotiate conditions that are more favorable. Most often, reasons for that lie in the original concluded contract, the parameters of which (primarily technical, license, and legal ones) make it more complicated to potentially switch to another supply company. The BIS identified several cases when the current contractor used illegitimate methods to win a new tender – and was usually given the necessary space to do so by a poorly set contractual relationship. Among such methods were efforts to gain inside contracting-authority information using established personal links, attempts to dissuade potential competitors from submitting a tender or to otherwise influence their decision-making, denial or obstruction of cooperation in a potential switch to another contractor, or intentions to misuse or influence inquiries of various bodies that conduct oversight of contracting authority's procedures. The state then often had to choose between prolonging existing unfavorable contracts, postponing a new tender, bearing high costs of the change of contractor, or facing the risk of legal consequences related to the effort to replace the original contractor. Most of the monitored cases pertained to large and technologically demanding projects. The contracting authority was in an exceptionally difficult position with respect to systems that were essential for the functioning of the state, which is something contractors could misuse to their own benefit.

Another type of past mistakes, the long-term consequences of which the state has to face, pertains to investment projects where cases of the contractor not complying with contractual provisions were not taken care of properly. The contracting authority, a state-controlled entity, was then unable to enforce the delivery of a functioning completed product or was forced to bear high costs of its completion. The BIS also identified efforts to mask past mistakes of persons responsible – e.g. by not enforcing contractual fines, which would effectively mean admitting the mistake. Representatives of the contracting authority were often indecisive and tended to postpone the solution with the aim of not being the one, who takes responsibility for the final, and often very

problematic, answer to complicated business disputes with contractors or debtors. Such cases pertained to the energy and transport sector.

Another type of monitored risks were legislation deficiencies pertaining to the conditions for activity in some sectors. These deficiencies then created scope for specific threats to state economic interests. A typical example was an arrival of a high-risk entity into a sector, where there were barriers to market access, but the rules did not cover all, sometimes quite new, risks sufficiently. In other cases, legal gaps or covert circumvention of the law were generally tolerated because they brought certain benefit to all participating entities, but to the detriment of the public budget as a whole. E.g. in the health sector, the BIS identified several weak points that private healthcare providers or service contractors used for their own financial benefit and the relevant state authority overlooked these situations because such a scheme helped to maintain financial stability of the system, albeit a very distorted one.

A common denominator of these risks was also the insufficient transparency in some sectors. Among other things, this insufficient transparency created alibi for entities responsible for oversight. However, the change in transparency of state-controlled entities in the most recent period can be assessed positively. Even though the BIS came across efforts of specific entities to circumvent in several cases rules of publishing information, the access to important data on the management of public funds is much better in comparison to the situation from a few years ago. The general view of what is a norm slowly reached the level when non-transparency itself causes suspicion of dishonest conduct.

System risks also arose from regulatory interventions that were a result of illegitimate lobbing to the benefit of sectional interests of some regulated entities. Decisions of regulatory authorities pertain not only to sector operation rules, but also to market access of individual participants, price conditions for trade in specific goods and services, or to the carrying out of strategic investments. Some private entities were partially successful in the effort to influence these decisions of regulatory authorities and the effort was aimed at imposing conditions favorable to these private entities or at suppressing competition. Interventions that harmed customers by resulting in the maintaining of conditions that were favorable to all regulated entities in a specific sector were serious.

In 2017, the BIS informed entitled addressees about cases of procurement by state-controlled entities that were of corruption nature. The identified cases did not pertain to top management of the state-controlled companies; organizers were usually in middle management or ran subsidiaries. When compared to the management of the whole group, these positions are not usually subject to sufficiently thorough oversight, which in some cases enabled the corruption system to function for several years.

What persisted was the risk arising from top representatives of important government authorities not having security clearance for the access to classified information. Some of these authorities are entitled addressees of the BIS. However, these institutions are not among entities, the representatives of which legally have access to classified information (e.g. the President of the Republic or Cabinet members). The only management member of such an institution, who has access to classified information, is usually the Director of the Security Section. Such situation creates a risk in cases when classified information of the BIS might be important to the operation of the given authority

but the absence of the security clearance by its decision-makers forms a barrier for effective sharing of such intelligence and decision-making on responses.

On the contrary, a positive trend was apparent by cartel agreements between those interested in contracts for transport infrastructure construction that the BIS pointed out repeatedly in past years. Market situation and a change in approach of procuring entities led to a partial elimination of scope for cartels, which seems to have a positive impact on costs in this investment segment.

Energy security remained an important topic. Many phenomena persisted that had a negative effect on state energy-security interests in 2016 already. Among them was active lobbing of private entities against essential infrastructure projects described in state strategic documents, efforts to influence regulatory decisions, or failures of some state-controlled companies in managing assets essential for the energy security of the Czech Republic.

Foreign companies from countries, where their strong ties to local state administration had to be expected, were constantly interested in important projects in the Czech energy sector. That caused risks linked to their potential participation in such projects because their participation could be used to promote foreign-political goals of their countries of origin, contrary to the interests of the Czech Republic.

2.2. Counterintelligence Activities

In accordance with the priorities, the threat level posed to the interests of the Czech Republic and the capabilities of the BIS, the main objectives were activities of Russian and Chinese state structures threatening the security and other key interests of the Czech Republic.

Russian activities continuously focused primarily on influence operations and witting and unwitting exploitation of Czech sources. Compared to the previous year, Chinese activities consisted of less influencing and more intelligence infiltrating in 2017.

The BIS did not identify any relevant activities of intelligence services of other countries with respect to its purview.

Russia did not change its extensive attitude towards using undeclared intelligence officers under diplomatic cover. Russian diplomatic personnel thus remain the most significant risk to Czech citizens of unintentional contact with a foreign intelligence officer and an instrument of pressure against the Ministry of Foreign Affairs of the Czech Republic, or more specifically the disproportionally smaller Czech mission in Russia.

For a long time, the size of the Russian diplomatic mission and the high number of individuals with affiliation to Russian intelligence services in the mission has been increasing the risks related to the reckless attitude of Czech citizens, primarily politicians and civil servants, towards unclassified, but inside, non-public information. It should be accepted that if the counterparty acquires enough unclassified inside information from a higher number of sources, it would not need to urgently steal classified information and that the fact that we consider someone only a diplomat does not mean that the individual does not pose risk or a problem.

The Czech Republic was a target of Russian activities that were a part of the general Russian hybrid strategy aimed against NATO and EU. However, the Czech problem is that “we do not see the

wood for the trees". The concept of hybrid conflict is based on a complex (combination ranging from a strict hierarchy/structure to a state of chaos) use of one's own available military and non-military instruments[1] (history, espionage, military operations, guerrilla, economy, organized crime, corruption, politics, information warfare, etc.), but also on the use of instruments or opportunities offered by the counterparty (e.g. freedom of speech). Individual segments or components of the hybrid strategy might only serve as a smoke screen to attract attention or create chaos – i.e. to draw attention away from other, essential components of the hybrid strategy. We therefore cannot fixate on selected component(s) of the hybrid strategy or campaign and we cannot perceive the Russian hybrid strategy only in the period starting with the Crimea crisis either.[2] What is essential is the goal of the Russian hybrid campaign – primarily to weaken NATO and the EU internally, e.g. by weakening individual member states.

<table>
<tr><td colspan="6">Russian hybrid strategy in short</td></tr>
<tr><td>1</td><td>(Pro)Soviet interpretation of modern history, enduring influence of Soviet propaganda</td><td>Continuous, latent,
Overton window[3]</td><td rowspan="3">Non-kinetic tools</td><td rowspan="4">Secrecy
Imitation
Simulation
Denial
Disinformation
Deception maneuvers</td><td rowspan="4">Establishing agendas, or more specifically using foreign-political agendas to influence internal policies of target states</td></tr>
<tr><td>2</td><td>Information warfare
• Information
• Disinformation
• Propaganda
• Deceptions</td><td>Ad hoc</td></tr>
<tr><td>3</td><td>Networking/infiltration
• Politics
• Economy
• Criminal sphere
• Espionage
• Culture
• Education</td><td>Continuous</td></tr>
<tr><td>4</td><td>Military/guerrilla operations</td><td>Ad hoc</td><td>Kinetic tools</td></tr>
</table>

The BIS therefore does not perceive so-called pro-Russian disinformation websites as a separate issue, but conducts intelligence work on Russian influence operations against the Czech

[1] These instruments can be used the way they are or they can substitute one another (an oligarch or a criminal authority carries out intelligence activities and vice versa; an intelligence officer acts like an academic and an academic acts like an intelligence officer; economic activities are not conducted for the purposes of business benefit, but political or military benefit, etc.).

[2] The Soviet Union lost the Cold War, but no one defeated Soviet propaganda or disrupted its enduring influence. Modern history presented in schools is de facto a Soviet version of modern history and even the education of the Czech language, or more precisely literature (National Revival), is influenced by pro-Russian pan-Slavism to a degree. The enduring influence of Soviet propaganda and the fact that Russians control modern history (Orwell: *He who controls the past controls the future. He who controls the present controls the past*.) form the basis for various current Russian influence operations and thus also for hybrid strategies.

[3] „You throw an internationalist out of the door and a campaigner against migration, Islamization, decadent chaos and defender of traditional Christian values comes back through the window."

Republic and its interests in a complex way. The BIS tried to filter away the ballast (the smoke screen) and identify (intelligence context is significant, not how much propaganda or disinformation the subject creates or distributes) key lines of Russian influence or infiltration operations (led in the context of politics, economy, nuclear energy, Ukrainian crisis, and the like), behind which stand Russian state structures or client structures linked to them.

The BIS perceives so-called disinformation websites only as one part of the Russian hybrid strategy system. In an overwhelming majority, disinformation websites are a part of the above-mentioned cover smoke screen, in which and behind which more significant activities linked to Russia and its interests hide. An overwhelming majority of disinformation websites in Czech are the work of Czech (ideologically motivated and convinced of the harmfulness of NATO, the EU, USA, and liberal democracy, or principally pro-Russian) citizens, who are not supported by Russian entities. Within their rights and freedoms, these activists only spread what they believe to be true. Their activities are a matter of discussion and critique within the freedom of speech and a potential civil litigation; however, we in no way dispute that these people and their internet projects are misused by Russia to spread propaganda or support other components of the hybrid strategy.

A specific issue that, however, fully corresponds with the Russian hybrid strategy is the counterintelligence view of Russian acquisitions of Czech private companies and Russian links to Czech cases related to corruption or other illegal activities. The nature of the issue lies in Russian investors (often represented by former members of Russian intelligence services) hidden behind Czech interposed individuals or off-shore companies taking property control of a Czech company that obtains or tries to obtain public contracts (including contracts of the so-called power ministries) and employs managers, who in the past played a part in cases investigated in the media or by the Police in relation to corruption activities. Identifying end owners of companies and identifying corruption activities in Czech state contract procedures is therefore important not only with respect to the danger to state economic interests, but also with respect to espionage risks – compromising information (threatening Czech individuals involved in corruption cases) might get to Russia via infiltrated contractors and subcontractors of Czech state structures (inside information on schemes of corruption cases and individuals involved therein).

In 2017, the BIS did not identify any strengthening of Chinese intelligence capabilities within the diplomatic mission in the Czech Republic. However, the intensity of intelligence activities of Chinese intelligence officers under diplomatic cover in the Czech Republic markedly increased, as well as intelligence activities against Czech targets conducted from China (including officers participating in ad hoc delegations coming to the Czech Republic). Given the high intensity of Chinese intelligence activities in the Czech Republic, the BIS believes that the risk of Czech citizens facing Chinese intelligence interest in China is extremely high.

Not only Chinese intelligence services were active in the Czech Republic or against Czech interests in a hostile way. Chinese career diplomats resorted to advancing Chinese interests in a coercive way as well. In this context, it is necessary to note that the Chinese approach is de facto just as hybrid as the Russian one – just like an intelligence officer, a career diplomat or a businessperson might pose a threat as well.

Chinese influence and intelligence activities conducted against Czech targets and interests can generally be divided into three segments: disruption of the single EU policy through Czech entities, intelligence activities aimed at Czech so-called power ministries, and economic, scientific and technical espionage.

The Chinese diplomatic mission also carried out measures that increased China's capability to monitor and control the Chinese compatriot community in the Czech Republic.

The BIS identified a worrying development in the area of Chinese activities (political, espionage, legislative, and economic) that as a whole pose a threat to the Czech Republic in the field of economic, scientific and technical espionage. China has almost unlimited funds at its disposal and is able to offer these funds to foreign companies in exchange for access to intellectual property or entry to foreign markets. China's interest is focused primarily on strategic economy sectors, such as energy, telecommunications, finance, logistics, health care, and cutting-edge technology. The Chinese government supports investments into these sectors. Its political goal, summed up in the ten-year "Made in China 2025" (MC2025) plan, is an independent and self-sufficient Chinese production. By 2025, China should become a global leader in the development and production of modern technologies. We consider the information and signals on several cases of Chinese activities against Czech legal entities to be a part of the Chinese effort to fulfil the MC2025 plan and the information and signals exhibit signs of economic, scientific and technical espionage.

2.3. Protection of the Constitutionality and of the Democratic Foundations of the Czech Republic

The BIS from its perspective did not identify any activities posing a specific and direct threat to the democratic foundations of the Czech Republic.

Similarly to previous years, the BIS focused on traditional extremism, i.e. groups and individuals, who espouse and promote classic totalitarian ideologies incompatible with the democratic legal order. However, more and more often the BIS was confronted with new phenomena that pose a threat to the democratic society and that have been emerging in the Czech and European politics in general in recent years.

The formerly majority area of the traditional political extremism linked to totalitarian ideologies faces a slowdown, numbers of its supporters dwindle and its appeal to the young generation is minimal. Partially, this is due to the continuous state security policy – a consequent anti-extremism policy forced supporters of these movements to act within the limits of the law and to adjust their behavior to the law. It is also the result of long-term enlightenment activities and the "collective memory of nations" that prevent the majority of the population from supporting groups adoring criminal totalitarian regimes and striving for their re-establishment. Finally yet importantly, the decline of these groups was influenced by the new socio-political reality of the beginning of the 21st century. The traditional right-left political division of society loses relevance today and society mobilizes and divides more on individual political issues. The existing demand for simple and quick solutions to difficult socio-economic problems also creates space that attracts not only "traditional" extremists, but also pure pragmatists, who address the issue primarily to satisfy their personal goals. The inflammatory language that accompanies the engagement of these extremists and pragmatists, however, contributes to further society polarization.

Anti-immigration and anti-Muslim activities

The anti-immigration spectrum was in crisis caused by not only its disunity, further splitting of groups, fights between individual activists, and unwillingness to cooperate, but primarily by the fact that the immigration topic faded away and ceased to attract public interest.

Because of the loss of mobilization potential, a considerable part of the anti-immigration movement gradually transformed into an "anti-government" movement. The majority of activists, who focused on the migration crisis after its beginning, turned their attention to any topics causing emotional reactions of the public, by means of which they could draw attention to themselves and gain as strong a support as possible among the population. A part of the spectrum, however, still tried to gain popularity by emphasizing the anti-Muslim language. They criticized primarily the incompatibility of Islam with the European culture and its alleged undemocratic and inhumane character or they openly called for an Islam ban.

The vast majority of this spectrum continued to declare publically its opposition to the Czech Republic remaining in the EU and NATO and took a positive stance towards President Putin's politics or emphasized the so-called Slavic mutuality.

Despite efforts to reflect various mobilization topics, the number of public events organized by anti-immigration/anti-government entities and their activities in general declined. Some activists even gave up their activities altogether.

These activities took the form of demonstrations, discussions with the public, petitions, leaflet campaigns etc. Compared to the previous year, these events were characterized by lower participant numbers and public involvement. In many cases, these events were only meetings of individual activists without political content. No dangerous protest forms were identified and the majority of radical displays was only verbal. Aside from their own events, activists also attended various protests organized by "common" citizens against some government decisions (against the registration of sales, against the ban on smoking in restaurants etc.).

The greatest risk of the activities of anti-immigration/anti-government entities continued to lie primarily in the spreading of fake or manipulated claims with the aim to criticize the establishment and contribute to the polarization and radicalization of a part of the public. In an extreme case, it might cause public distrust in the existing system and lead to society destabilization.

A problematic security aspect related to representatives of this spectrum was still their strong pro-Kremlin orientation, because of which the risk remained that they might be used by Russian entities to advocate their interests to the detriment of the democratic foundations of the Czech Republic.

Paramilitary and militia groups

Activities of paramilitary and militia groups did not pose a real direct threat to the democratic foundations and security of the Czech Republic. They did not radicalize or use violence more intensively. On the contrary, their activity and security potential decreased because of a number of reasons.

One of the main reasons was the loss of mobilization potential because of the marginal impact that the migration crisis had on the Czech Republic. Paramilitary and militia groups were created primarily because of the declared fear of the arrival of Muslim refugees and the subsequent

deterioration of the security situation. The nearly zero arrival of migrants to the Czech Republic therefore led to a decrease in public interest in this issue and thus also to a decrease in the support of paramilitary and militia groups and to their general weakening. Their membership became smaller, there were fewer active members, and there was a decline in activities and a decrease in the number of public events organized by them and in the number of people who attended them.

Compared to the previous year, paramilitary and militia groups did not primarily try to create the impression that Czech security forces were incapable of protecting the country and its citizens. On the contrary, some of the groups strived to become partners in the protection of state security. Their representatives tried to legalize militias by enshrining this instrument in the Czech legal order or tried to establish official cooperation with representatives of cities, towns, and villages in the area of security protection in order to legitimize their activities. Self-promotion activities of these groups, efforts to improve their media image and to gain public sympathy and support were related to that.

The ongoing efforts to arm paramilitary groups were connected to the society-wide trend of an increased interest in obtaining firearms licenses and holding firearms and to the intention of the Ministry of the Interior to enshrine in the Czech constitutional order the right to use a firearm for protection against terrorism.

Probably the most problematic security aspect arising from the activities of paramilitary and militia groups was their pro-Russian orientation. Because of that, the risk remained that they might be misused to spread pro-Russian propaganda, influence and destabilize the security situation in the Czech Republic, or to advocate other goals of the policy of Russian President Putin.

Right-wing extremism

Activities of the traditional right-wing extremist scene did not pose a more significant risk with respect to political significance or security threats. Representatives of the scene have been facing a crisis for several years.

The popularity and support of politically engaged right-wing extremists was minimal. That was reflected in the result of parliamentary elections that ended in complete fiasco for them. On the other hand, populist entities or (at least on the outside) mildly radical entities managed to attract the interest of right-wing extremist voters.

The significance of the neo-Nazi and ultranationalist scene diminished as a whole, but the threat of individuals, who are not organized formally, or small groups inclined to violence or more open right-wing extremism grew, especially with respect to their disunity and low level of institutional organization.

As the right-wing extremist scene transformed, its main topics changed as well. Aside from the lessening anti-immigration activities and anti-Islam events, right-wing extremists focused on other goals as well, e.g. on the criticism of the EU, protests against the existing political representation, and distancing themselves from human-rights activists or non-governmental organizations. In many cases, they were in agreement with nationalists from the left-wing extremist scene. The most distinctive manifestation of that was the positive view of the politics of Russian President Putin, but also e.g. the rejection of the membership of the Czech Republic in NATO or the negative attitude towards Israel.

While the Czech right-wing extremist scene still partook in anti-Muslim and anti-immigration language to a certain degree, there were no serious physical attacks, which also shows the dismal state of the scene and its relative moderation. The largest space for hate speech was the internet and in an

overwhelming majority, such statements were expressed by individuals, who cannot be termed right-wing extremists.

Contacts between Czech and foreign right-wing extremists had various forms, e.g. reciprocal participation in public events or attendance at concerts. The main partners of Czech extremists were their counterparts from Slovakia, Germany, and Poland.

Right-wing extremist events with music continued to be held. Their character usually was not openly right-wing extremist. Various smaller private events were an exception and their participants often did not shy away from openly neo-Nazi displays. Concerts abroad remained popular, mainly in Slovakia and Poland.

Left-wing extremism

The left-wing extremist scene did not pose a security threat to the democratic foundations of the Czech Republic. It remained strongly fragmented, lacked distinctive figures to unite it, and the membership of its platforms remained weak. Its supporters sidelined their public activities and focused on organizing various smaller-scale events aimed at the movement itself.

One of the main mobilization topics for anarchist-autonomous and Trotskyist groups was still the support of squatting. The group around the Autonomous Social Center Clinic (Clinic; in Czech: *Autonomní sociální centrum Klinika*) ignored the court decision and continued to illegally inhabit the property of the Railway Infrastructure Administration (in Czech: *Správa železniční dopravní cesty*). Clinic thus remained a place for activities and meetings of sympathizers from a broad spectrum of the far left, but also various human-rights activists. Aside from that, Clinic was also a significant element in the development and strengthening of international relations of the Czech far left scene.

Anarchist-autonomous activists newly focused more on environmental protection and environmental activism that gradually became another one of their profiling topics. Their links to various environmental activist groups not only in the Czech Republic, but also in Germany were apparent. They attended events organized by these entities or even participated in the organization.

The BIS did not identify any direct operations claimed by militant anarchists. Individuals charged with the preparation of an attack on a train with military equipment were acquitted by as of yet non-final decision of the Prague City Court from September 22, 2017. In 2017, some of the individuals still associated with left-wing extremists, but they were not markedly active, with the exception of a few activists, who had been in custody and after their release shared their prison experience at various lectures and talks.

In comparison to previous years, the traditional fight of anti-fascists against right-wing extremists was sidelined. One of the main reasons was the minimal public activity of far right entities. The anti-fascist spectrum therefore focused more on protests against right-wing populists.

The refugee crisis did not constitute a very significant mobilization topic for left-wing extremists anymore either. Pro-immigration activities were on the decline primarily because the international situation has so far quieted down and migration opponents did not emphasize the issue further.

Within the framework of international cooperation, a part of the left-wing extremist scene was interested in protests against the G-20 summit (Hamburg, July 5 – 9, 2017). Several Czech anti-authoritarians participated in the event and were detained during the protests.

The radically communist part of the left-wing extremist scene stagnated; its representatives were essentially inactive. Trotskyist groups were still very fragmented; their membership remained small. Some of them cooperated with anarchist-autonomous groups to a degree, others preferred to cooperate with young communists.

2.4. Terrorism

The BIS looked into potential links of the perpetrators of terror attacks in the EU to the Czech Republic, and did not register a direct threat of a terror attack in our country.

The BIS also focused its efforts on obtaining information on foreign fighters who left the national territory to join the fight in the Middle East as members of terrorist organizations. The number of foreign fighters linked to the Czech Republic increased to eleven people in 2017, including two Czech citizens. Other findings confirmed departures of foreign fighters in previous years, as well as their activities in the Middle East. The BIS shares identities of foreign fighters within interagency and international counterterrorism cooperation in all cases.

As concerns detecting signs of radicalization, the BIS focused inter alia on communities originating from the Islamic world that may pose a potential threat. In the first place, the issue concerned members of a closed ethnic community from Central Asia. Certain members joined the efforts to spread Islamism in the EU by establishing networks of personal and online contacts.

Terror risk assessment concerned also Maghrebis residing in the Czech Republic, mainly because people of Maghrebi origin amply participated in terror attacks on the European continent. Poor integration of this group makes the Maghrebis a part of Muslim population that can be easily radicalized in Europe, including in the Czech Republic. Islamist recruiters in European states often approach young men with personal issues because they tend to accept radical interpretations of Islam, as well is the ideas blaming the Western civilization for their problems more smoothly.

Pakistani and Afghan communities included people organizing illegal migration. Their activities posed risks by, among other things, allowing for a facilitated entry of migrants from the Islamic world to the Schengen Area. Potential terror attack perpetrators or future Islamic radicals might have been present among the migrants. For a similar reason, the BIS focused on the stays of the so-called Libyan patients who travelled to the Czech Republic within a Libyan state-funded medical program. Due to a poor security situation in Libya, with activities of terrorist organizations and fighting of numerous Islamist militias, there was a danger of abuse of the program by Islamist radicals.

When revealing and monitoring potentially dangerous phenomena within the circles of Muslims living in the Czech Republic, the BIS obtained information on people whose behavior showed radical traits. Their actions did not lead to further risk activities and did not influence the moderate character of the Czech Muslim community as a whole.

In addition to the aforementioned topics, the BIS obtained findings on ethnic communities of Middle Eastern origin, for which the ethnic affiliation served as the main unifying element.

As concerns Kurds posing a potential threat and living in the Czech Republic, the BIS focused on activities of Kurdistan Workers' Party (PKK), a terrorist organization, in the Czech Republic. The PKK activities in the Czech Republic have been futile over a long period due to the absence of unconditional support by the local Kurdish community. There are no PKK members among the Kurds living in the Czech Republic, only its supporters, and the Party does not have its official representation in our country, nor a fixed organizational structure. A demonstration to support the Kurdish independence, inspired by a planned referendum in the Iraqi Kurdistan, did not change the situation.

In the context of the Syrian civil war, the BIS did not notice a strong reflection of the issue into the life of Syrian diaspora in the Czech Republic. Activities of the Syrian Sunni exiled opposition have been going through a long-term decline, which was reflected also in the developments in our country. On the contrary, a space for propaganda by the supporters of the Bashar al-Assad's regime abroad appeared. Also due to its diplomatic mission in Damascus, the Czech Republic has become popular among certain senior Assad's regime representatives and their children studying in the Czech Republic, as a relax zone and entry point to the Schengen Area. No terror-related risks appeared in connection to their stays in the Czech Republic.

The BIS focused also on the Iranian intelligence activities in the Czech Republic. Certain people are obviously ready to act for the benefit of the Iranian regime, including by efforts to engage in propaganda activities for the benefit of the regime and its security forces, the Islamic Revolutionary Guard Corps (IRGC). Some activities may correspond to the interest of the Iranian intelligence services to penetrate Iranian anti-regime opposition.

The Iranian regime seeks to establish business and political relations in the Czech Republic. Therefore, also the people associated with the Iranian security forces and its regime come to our country.

2.5. Proliferation of Weapons of Mass Destruction

As a member of all the International Control Regimes (ICRs)[4], the Czech Republic has made a commitment to minimize risks related to international trade in conventional weapons, military material, explosives and dual-use goods and not to participate in proliferation of weapons of mass destruction and their carriers (WMD). Nuclear, chemical and biological (bacteriological and toxin) WMD are excluded from trade in the Czech Republic, and other internationally controlled items are subject to legal provisions[5].

Despite that, the states posing the gravest threat (DPRK, Syria and Iran are still among them) were interested in specific engineering devices, special materials, technologies and know-how that may be used for research and development of their own WMD. They projected complex trade routes via third countries to obtain goods with required technical parameters. They managed to involve front

[4] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (WA), Australia Group (AG), Missile Technology Control Regime (MTCR), reinforced by The Hague Code of Conduct (HCOC), Nuclear Suppliers Group (NSG), Zangger Committee (ZC), and United Nations Security Council Resolution No. 1540 (2004).

[5] E.g. Act No. 38/1994 Coll. On Foreign Trade with Military Material; Act No. 594/2004 Coll. Implementing the European Community Regime for the Control of Exports of Dual-use Items and Technologies; or Act No. 61/1988 Coll. On Mining Activities, Explosives and the State Mining Administration, as Amended.

companies and entities, which were often unaware of the real purpose of the trade and of the extent of other companies' involvement. In order to thwart possible identification of the trade routes and companies involved, they tailored the payments for goods to the complex trade routes.

International community uses sanctions against such efforts of states that may pose proliferation risks. The sanction measures ban supplies of controlled items, as well as acceptance of payments for such trades. The UN Security Council enforced sanctions against DPRK for its missile and nuclear tests by four Resolutions in 2017. The sanctions against Syria remained in force. Despite lifting sanctions against Iran in nuclear area, measures banning supplies of conventional weapons and goods for the missile program remained in force. Since August 2014, the EU sanctions have affected also the supplies to Russian arms factories and entities with arms programs. Numerous arms sanctions were imposed on certain states in the Middle East, Southeast Asia, Caucasus and Africa.

Arms embargoes pursuant to the UN Security Council resolutions, (EU) Council Regulations or to the Organization for Security and Cooperation in Europe (OSCE) significantly limit trade with such states, or ban them completely. States with instable or repressive regimes or states in armed conflicts expressed interest in military material, weapons and explosives or in special components, which may serve to develop and produce e.g. unmanned aerial systems for military purposes. Violation or circumvention of sanctions would jeopardize the good reputation of the Czech Republic at the international level.

Being a traditional manufacturer of engineering devices, materials and technologies at international level, the Czech Republic was approached with demands for goods that may be used for proliferation purposes. Measures against circumvention of the control regimes made use of continuous assessments of partial findings about developments in companies and their business partners and about preparation and conducting of trades, and information exchange, including at international level. Despite that, some businesspersons believed that concealing the real purpose of the trade, e.g. by declaring civilian use of the exported goods, would help them obtain an export license. Such steps and similar methods damaged the good reputation of the Czech Republic and its exported-related activities.

In a timely manner, the BIS informed entitled addressees about particular events, phenomena and trends associated with foreign trade in controlled items, including about evading or non-compliance with other obligations of the Czech Republic, arising from sanctions against specific states or entities[6] as provided for in law.

2.6. Cybersecurity

Cyber espionage

2017 was marked by cyberespionage against the Czech Republic. In terms of extent and consequences, the most significant case was the compromise of a Ministry of Foreign Affairs (MFA) information system. Detected in the beginning of 2017, the compromise had lasted at least since the beginning of the previous year.

The MFA electronic communication system had been compromised at least since the beginning of 2016 when the attackers accessed more than 150 mailboxes of the MFA staff and copied

[6] Section 5, Paragraph 4 of Act No. 153/1994 Coll. On the Intelligence Services of the Czech Republic.

emails, including attachments. They thus obtained data that may be used for future attacks, as well as a list of potential targets in virtually all the important state institutions. The attackers focused mostly on mailboxes of top ministry representatives. They accessed their mailboxes in a repeated, long-term and irregular manner.

The case of mailboxes compromise in numerous key aspects corresponds to similar cases of cyberespionage, which took place in other European states over the same period.

In parallel with this cyberespionage attack, an attack against mailboxes of the same Ministry was underway since December 2016. This time, attackers strived to guess the login details of mailboxes by brute force (the so-called brute force attack), and made thus efforts to compromise several hundred mailboxes.

Most likely, those two incidents were not interrelated. All the findings make it clear that it was the Turla cyberespionage campaign, originating from the FSB, a Russian intelligence service, and APT28/Sofacy, which is credited to the Russian military intelligence, the GRU.

Russian APT28/Sofacy was among the most active cyberespionage campaigns. It does not focus on data alone, but increasingly also on theft of personal data and login details for information and communication systems. Such data may be used for later sophisticated spearphishing[7] attacks.

As in 2016, it was probably the most active and most visible Russian cyberespionage campaign. APT28/Sofacy used foreign computer infrastructure for its attacks against Czech targets.

In connection to the campaign, the BIS detected several attacks against Czech military targets. The most serious included compromising of several private email accounts of people linked to the Ministry of Defense and the Army of the Czech Republic and compromising of an IP address belonging to the Ministry of Defense/Czech Army by a malware known as X-Agent. Although the attackers most likely did not obtain any information, which are considered classified pursuant to Act No. 412/2005 Coll., they obtained numerous personal information and sensitive data that may be used for further attacks and illegitimate activities.

The wave of spearphishing emails targeted mainly people from military diplomacy deployed in Europe. Vector and targets of this attack fully corresponded to the mode of the attack and the sphere, primarily targeted by the Russian APT28/Sofacy campaign. A similar spearphishing attack targeted also European arms companies and a border guard of a European state.

In addition to cyberespionage cases, the BIS also detected IP address ranges with servers and domains used for criminal activities or cyberespionage purposes.

At the beginning of 2017, the BIS learnt about insufficient security of a web portal of another Czech Ministry. At a subdomain of the Ministry portal, it was possible to obtain information about server configuration and certain login data via possible manipulation with URL links. The web portal was also vulnerable to SQL injection-type attacks, which might have been used to penetrate

[7] Spearphishing emails look like mails from someone known and trusted by the recipient (friend, superior, employer, business partner, and so on). They often use social engineering methods in the content of e-mail.

illegitimately the database and to compromise or impair saved data. The BIS immediately informed the Minister concerned and the National Security Authority Director, as the then guarantor of cybersecurity in the Czech Republic.

Visapoint

The BIS continued to deal with persisting problems of the Visapoint information system, a system exploited by visa intermediaries for unauthorized financial benefits. Despite the MFA's efforts - in cooperation with the system provider - to eliminate the deficiencies and to limits its use, numerous issues persisted. System functionality was limited over a long period of time, which allowed the intermediaries to block and subsequently to sell available dates for personal appointments at the Czech embassies. Consequently, the issue led to damaging of the reputation of the Czech Republic in international context. Due to the persisting issues, among other reasons, the operation of the system was ceased in October 2017.

3. Protection of Classified Information

3.1. Administrative Security

The BIS drew up expert opinions related to protection of classified information and expert studies on classification in accordance with Act No. 412/2005 Coll. and interpreted items listed as classified in the BIS sphere of powers and responsibilities, both in reply to internal requests and requests from state administration authorities and other institutions.

Current legislation does not provide sufficient and effective protection of classified intelligence in the administrative procedure and in the potential subsequent judicial review. However, this is an essential and necessary precondition for intelligence services to provide relevant information in a form enabling its further use by an administrative body. The BIS has been repeatedly drawing attention to this issue, which is related to incomprehensive and inconsistent regulations of various administrative procedures. These procedures are governed by special legislation and in/directly anticipate the use of intelligence findings.

3.2. Security of Information and Communication Systems

All BIS information systems processing classified information have a valid National Cyber and Information Security Agency (in Czech: *Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB*) certificate. Security documentation was updated and information system for processing classified information as Confidential was successfully re-certified.

Further advanced technologies for tracking user access to data were tested. After assessment of tests, the BIS will implement the technologies to its systems to enhance the security of processed information.

The BIS detected no serious security incidents in the operation of information and communication systems or compromising of cryptographic devices

3.3. Physical Security

In the area of physical security, the BIS implemented measures aimed at improving special rules systems providing for the operation of BIS buildings, their technical protection and their physical guarding in order to meet the requirements on the protection of classified information provided in Act No. 412/2005 Coll. and in Regulation No. 454/2011 Coll.

Documentation on BIS offices and buildings was regularly updated by new mandatory parts. Due to the relocation of some workplaces, relevant documentation was amended to reflect the current situation.

3.4. Crisis Management

Focusing on the protection on classified information in emergencies, Plans for Building and Area Security, which are part of Security Projects, were updated.

4. Cooperation with Intelligence Services of the Czech Republic and with other State Authorities

4.1. Cooperation with Intelligence Services of the Czech Republic

The BIS regularly provides intelligence and findings to the Military Intelligence and the Office for Foreign Relations and Information. Cooperation with these services takes place at different levels encompassing operational, analytical and service activities.

Close cooperation with the Office for Foreign Relations and Information and with the Military Intelligence focused on counterespionage and on fighting WMD proliferation and the illegal trade with military material.

Countering terrorism is a specific part of cooperation. The BIS cooperated on counter-terrorism with the two intelligence services of the Czech Republic and other state authorities and security forces – either bilaterally or working together in the Joint Intelligence Group and in the National Contact Point for Terrorism (in Czech: *Národní kontaktní bod pro terorismus – NKBT*).

4.2. Cooperation with the Police of the Czech Republic

The BIS played an active role in regular meetings of the National Contact Point for Terrorism (in Czech: *Národní kontaktní bod pro terorismus*) falling under the remit of the National Centre against Organized Crime (in Czech: *Národní centrála proti organizovanému zločinu*).

Section 8, Paragraph 3 of Act No. 153/1994 Coll. stipulates that the BIS must provide information to the Police of the Czech Republic if this does not jeopardize an important intelligence interest. Under Section 8, the BIS also provides the information to the President, the Government, the Prime Minister and other Cabinet Ministers. In many cases, cooperation between various departments of the BIS and the Police draws on the nature of submitted information.

Effective bilateral cooperation on individual cases took place with relevant police units, in particular with specialized units.

The BIS and representatives of the Criminal Police and Investigation Services focusing on investigating economic crime attended meetings regarding organized crime activities in the Czech Republic. The meetings focused on advocacy groups, corruption, fund transfers among organized crime groups, and on organized crime infiltrating public administration.

The BIS and the respective departments of National Centre against Organized Crime discussed dysfunctional public and local administrations, organized crime infiltrating public administration, and individual persons and advocacy groups of interest. The BIS cooperated with the Centre also on cases of electronic attacks.

The BIS continued to cooperate with the Police of the Czech Republic on issues regarding illegal trade and manipulation with military material, security material, guns, ammunition, explosives and with hazardous materials, and on fighting WMD proliferation.

In the area of physical security, the BIS has cooperated with the Police of the Czech Republic on security guarding of the BIS buildings.

4.3. Cooperation with other State Authorities and Institutions

Close cooperation of the BIS and the National Security Authority on protecting classified information continued. The cooperation involved mainly the following investigations based on NBÚ requests: investigations pertaining to personal and industrial security and security clearance and security clearance examinations examining whether a natural or legal person holding security eligibility certificates still meets the requirements for their issuance. Throughout the year, meetings regarding the cooperation on specific issues were held.

In addition to activities on NBÚ requests, the BIS provides information indicating that a holder (natural or legal person) of a security clearance or security eligibility certificate no longer meets the requirements set for the holders thereof. In accordance with Section 8, Paragraph 3 of Act No. 153/1994 Coll., or Section 140, Paragraph 3 of Act No. 412/2005 Coll., the information is passed to the NBÚ, or if the information concerns employees or officials of intelligence services, to the services concerned. The BIS also routinely pass information in reaction to numerous and repeated NBÚ requests on possible information on holders of security clearance or security eligibility certificate (requests pursuant to Section 107, Paragraph 1, Section 108, Paragraph 1, and Section 109, Paragraph 1 of Act No. 412/2005 Coll.).

Furthermore, efforts to improve and broaden cooperation on enhancing cybersecurity, in particular with the National Cyber and Information Security Agency.

The BIS cooperated also with Czech custom authorities – the Directorate General of Customs (in Czech: *Generální ředitelství cel – GŘC*) and local customs directorates – on fighting WMD proliferation. Cooperation in the fight against WMD proliferation took place also with the Ministry of Foreign Affairs, the Ministry of Industry and Trade Licensing Administration, and with the State Office for Nuclear Safety (in Czech: *Státní úřad pro jadernou bezpečnost*) and its subordinate organizations.

The BIS cooperated and also with the following state bodies regarding various spheres of interest (banking, the management of state funds and assets, economic competition, protection the Czech Republic from the influence of foreign intelligence services): the Cabinet Office, the Czech National Bank, the Financial Analytical Unit (in Czech: *Finančně analytický útvar – FAÚ*), the General Financial Directorate (in Czech: *Generální finanční ředitelství – GFŘ*), the Directorate General of Customs, the Prison Service (in Czech: *Vězeňská služba*), the General Inspection of Security Forces (in Czech: *Generální inspekce bezpečnostních sborů – GIBS*), the Supreme Prosecutor's Office in Prague (in Czech: *Vrchní státní zastupiteltství v Praze*), and the Office for the Protection of Competition (in Czech: *Úřad pro ochranu hospodářské soutěže*). Regular consultations of the issues with those bodies were held.

The BIS Inspection Department cooperated with other public administration bodies primarily in connection with requests sent by police bodies engaged in criminal or misdemeanor proceedings. The requests did not involve BIS officials. They were related to information the police bodies needed for their work and were not able to obtain by themselves. The number of these requests does not undergo significant changes.

The BIS cooperated also on projects of other state authorities (e.g. Ministry of the Interior and Ministry of Foreign Affairs) contributing to the protection of the interests of the Czech Republic and its citizens and to limiting or eradicating security threats. The BIS processed requests related to tens of thousands of natural and legal persons.

In 2015, an amendment of Act 49/1997 Coll., on Civil Aviation, which stipulates provisions regarding reliability certificates issued to natural persons by the Civil Aviation Authority, came into force. These screenings include a credibility assessment of the natural persons conducted by the Police of the Czech Republic. Based on Police requests for cooperation in assessing credibility, the BIS gave opinion on applicants for the Civil Aviation Authority certificates.

The BIS is also an active member of the Joint Intelligence Group, a permanent working body of the Committee for Intelligence Activity, contributing to the cooperation and exchange of information between the BIS, other intelligence services and state authorities.

In addition to providing and exchanging information, the BIS provides other state authorities with generalized findings and recommendations when commenting on various legislative and non-legislative documents. Furthermore, the BIS organizes various training courses, holds consultations, etc.

Expert opinions related to the protection of classified information were drawn up within the BIS, on requests by state administration authorities and other entitled institutions.

The BIS representatives took part in meetings of National Security Council working bodies – Committee for Coordination of Foreign Security Policy, Committee for Domestic Security, Committee for Intelligence Activity, Committee for Defense Planning and Committee for Civil Emergency Planning – and their subcommittees and working groups. Recommendations and opinions were drawn up on materials of the National Security Council and its committees.

Crisis management office intensely cooperated with state administration central authorities, mostly with the Ministry of Defense, Ministry of the Interior and Administration of State Material Reserves.

5. Cooperation with Intelligence Services of Foreign Powers

Cooperation with intelligence services of foreign powers is provided for in Section 10 of Act No. 153/1994 Coll. The BIS is authorized by the Government to cooperate bilaterally with over a hundred of intelligence services. In 2017, the BIS actively cooperated with around two thirds of them. As far as multilateral cooperation in 2017 is concerned, the BIS was active in several organizations, e.g. Counter-Terrorist Group or NATO Civilian Intelligence Committee.

The BIS received almost 10 000 reports from its foreign partners and sent almost 2 000 documents. BIS representatives took part in more than 700 international strategic and expert meetings.

Compared to 2016, international information exchange again increased.

The cooperation continued to focus mostly on the fight against terrorism, counterintelligence, proliferation and cyber security. The main partners in terms of international cooperation are the intelligence services of the EU and NATO Member States and of some other states.

6. Oversight

Act. No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, provides a legal basis for the oversight of intelligence services. Section 12 of this Act stipulates that the activities of intelligence services are subject to oversight by the Government and Parliament, and with effect from 1 January 2018, also by the Independent Authority for the Oversight of Intelligence Services of the Czech Republic. Furthermore, this Act (Sections 14 – 16) defines the relation between the Chamber of Deputies (lower house) of the Czech Parliament and the Government as far as intelligence services are concerned. Moreover, Section 12 refers to a separate Act providing for direct parliamentary oversight of intelligence services. Section 13a provides for specific oversight conditions.

The Act defines neither the scope nor the manner of government oversight. It is based on the Government's entitlement to assign tasks to the BIS within the Service's legal powers and responsibilities and to assess their fulfillment; and on the fact that the BIS is accountable to the Government, which also coordinates its activities and appoints and dismisses the Director of the BIS. Section 8, Paragraph 1 of Act No. 153/1994 Coll. states that the BIS must submit reports on its activities to the President and to the Government once a year and whenever it is requested to do so. Government oversight focuses on all BIS activities.

Sections 14 to 16 of Act No. 153/1994 Coll. regulate information provided by the Government to the Chamber of Deputies. Section 14 stipulates that the Chamber of Deputies is informed about the activities of Czech intelligence services by the Government, through the intermediation of its respective body for intelligence services. Direct parliamentary oversight of intelligence services as stipulated by Section 12 of Act No. 153/1994 Coll. is defined by separate legislation; therefore, the above-mentioned respective body for intelligence services acts to a certain extent as a means of parliamentary oversight of the Government.

The separate legislation mentioned in Section 12 of Act No. 153/1994 Coll. is Act No. 154/1994 Coll., on the Security Information Service, as amended. Under Section 18 of the said Act, the responsibility for overseeing the activities of the BIS lies with the Chamber of Deputies, which sets up a special oversight body - the Standing Oversight Commission. Sections 19 and 20 of the said Act provide specifically for the particular powers of the Oversight Commission. Authorized members of the oversight body may, e.g., enter BIS buildings when accompanied by the BIS Director or by a BIS official designed by the Director for this purpose; or request due explanation from the BIS Director should they feel that the activities of the BIS illegally curb or harm the rights and freedoms of citizens. The Director of the BIS is obliged to provide legally defined information and documents to the Oversight Commission.

Oversight regarding BIS management of state-assets and of the funds allocated to the BIS from the state budget is stipulated in Act No. 320/2001 Coll., on Financial Audit in Public Administration and on the Amendments to some Acts (the Financial Audit Act), as amended, and in Regulation No. 416/2004 Coll., implementing this Act. Internal audit activities are provided for in an internal regulation issued by the Director of the BIS.

6.1. External Oversight

Authorities and institutions with the legal right to oversee individual activities of the BIS carry out external oversight of the BIS. In 2017, 4 external audits were conducted - an audit of public health insurance and other obligations of insurance payer, audit of compliance with obligations from health insurance, pensions and from payments of insurance for social security and contribution to state employment policy, and two audits of protection of public health and food hygiene.

6.2. Internal Audit

The BIS internal audit service operates in compliance with Act No. 320/2001 Coll., on Financial Control in Public Administration and on the Amendments to some Acts (Act on Financial Control), as amended. Its scope of powers and responsibilities is set by the organizational structure and internal regulation by the BIS Director. In 2017, the internal audit service carried out audits in compliance with the annual work plan focused on commissioning public tenders, internal control system and on implementation of recommendations approved by the BIS Director.

Other BIS expert units conducted 52 inspections. These inspections focused on compliance with internal regulations in respect to economical and effective management of individual BIS departments. The inspections focused on the following areas:

- fulfillment of the budget; adherence to binding limits and the keeping of records; management of means of respective material categories; adherence to direct acquisition principles; use of meal allowances and keeping records;
- provision of material needs in organizational units and keeping material records;
- monitoring the technical condition of vehicles; management of fuel consumption; use of vehicles and keeping relevant records;
- use of buildings in accordance with their intended purpose; adherence to norms for accommodation and for the operation of buildings; adherence to the principles of occupational safety, health protection, hygiene, fire protection, water management, and of ecology; monitoring energy consumption;
- the equipment of buildings with security technologies and the effective use of the installed security technologies.

The inspections did not reveal any serious shortcomings. Detected shortcomings (mostly of administrative nature) are eliminated immediately or gradually within set deadlines.

In compliance with Section 76 of Act No. 187/2006 Coll., on Sickness Insurance, the BIS carried out 13 inspections of persons (officially on a contract of service and former officials in the protection period) temporarily unable to work.

Employees of the archive and of the control group carried out 52 archive inspections related to records management. The inspections focused mainly on establishing that no classified documents or their parts were missing, on meeting administrative requirements, and on the precision of keeping record entries.

Intelligence documentation stored by individual BIS divisions and documentation stored in the registry was regularly inspected.

As far as physical security is concerned, the following inspections were carried out: adherence to requirements for the storage of classified documents, and inspections of installed security elements at the BIS buildings, including of security lock systems.

7. Maintenance of Discipline; Handling Requests and Complaints

The work of the BIS Inspection Department is based on laws on intelligence services, Code of Criminal Procedure, and on internal BIS regulations.

The BIS Inspection Department activities can be divided into four main areas:

- Acting as the BIS police authority within the meaning of Section 12, Paragraph 2 of the Code of Criminal Procedure, on suspicion of commitment of a criminal act by a BIS official;
- Investigation of conduct suspected of having the traits of a misdemeanor and of a disciplinary infraction by a BIS official, including emergencies;
- Investigation of complaints, notifications and motions by the BIS officials and external entities;
- Processing requests submitted by other law-enforcement authorities in accordance with the Code of Criminal Procedure and requests by other state administration authorities. The BIS Inspection Department cooperates with other state administration authorities in relation to requests sent by the Police authorities involved in criminal or misdemeanor proceedings. The number of those requests does not undergo significant changes.

7.1. Investigation of Conduct Suspected of Having the Traits of a Misdemeanor, of a Disciplinary Infraction, and of other Infractions

In this area, the BIS Inspection Department focuses on traffic accidents involving Service officials (accidents both caused and not caused by BIS officials). The Inspection Department is responsible for findings that cannot be provided by the Police but are important for a decision in the matter. Further, this category includes investigation of matters related to the protection of classified information, incidents related to the health of BIS officials and conduct suspected of disciplinary infraction or other infractions.

Cases of conduct suspected of disciplinary infraction or of having traits of a misdemeanor by a BIS official were referred to a disciplinary proceeding.

7.2. Investigations of Complaints and Notifications

In 2017, the BIS Inspection Department investigated complaints, notifications and suggestions submitted mostly by external entities. Compared to 2016, the number of notifications and suggestions decreased by 5.8%, and only one submission was declared a complaint. In terms of content, reports made by citizens reflected society-wide developments in the Czech Republic and abroad.

8. Budget

The budget of the BIS was stipulated by Act No. 457/2016 Coll., on the State Budget of the Czech Republic for 2017.

Salaries and equipment payments accounted for the majority of total expenditures reflecting the importance of people for an intelligence service. Personnel expenditures also include severance benefits, i.e. mandatory payments for Service members whose service has ended.

Further current expenditures included mainly standard expenditures for services, fuels and electrical power expenses ensuring the normal functioning of the organization. Expenditures for repairs and maintenance aimed at assuring the appropriate technical condition of the property and buildings of the BIS. Furthermore, funds were allocated for intelligence technology and field intelligence activities.

A significant part of capital investment expenditures was invested in modernization of information and communication technologies and intelligence technology development.

Another part of capital investment expenditures was allocated to construction investments. Due to the time and administrative complexity of relevant procedures to meet all deadlines and procedural rights of parties involved, a part of expenses for actions launched in 2017 will be transferred to the following year.

The budget reflects requirements on the protection of classified information provided for in Act No. 412/2005 Coll., especially in the areas of physical, administrative, and personnel security, and in the area of security of information and communication systems. The need to take these facts into consideration in the whole spectrum of BIS activities leads to much expenditures, which are absent or very limited in other organizational units of the state.

Budget allocated to the BIS Section in 2017 allowed covering basic operational needs. In terms of personnel, the budget improved and allowed 5% increase in the number of occupied Service posts compared to the previous year. The budget also financed development of intelligence technology and information and communication technologies.

Indicators of Budget Section 305 – Security Information Service in 2017 (thousands)

	Approved budget	Amended budget	Real data
Total revenues (CZK)	146 700	146 700	174 252
Total expenditures (CZK)	1 652 946	1 692 907	1 370 905

A detailed analysis of BIS economic management structure in accordance with the relevant regulation of the Ministry of Finance of the Czech Republic is submitted to the Ministry of Finance and to the Security Committee of the Chamber of Deputies of the Czech Parliament.