Annual Report of the Security Information Service for 2019

Table of Contents:

A Message from the Director General of the Security Information Service

Dear Readers,

Continuing a tradition of twenty-four years, the Security Information Service (BIS) provides the general public with an unclassified edition of its Annual Report on the Activities of the Security Information Service for 2019.

As in the previous years, we believe that the Annual Report will inspire a great deal of interest and lead to numerous debates regarding not only each and every of its chapters, but also the reasons why the BIS should publish a freely accessible report. On many occasions, I have pointed out my belief that it is equally important that our work is overseen by the Government and Parliament of the Czech Republic as well as by the general public. Czech citizens should be aware of the phenomena and threats the BIS focused on in 2019 and be given information on what were the Service's priorities and how they were specified, which organisations the BIS cooperated with and what information was delivered to the entitled addressees, including the Prime Minister, Government members, President and law-enforcement authorities.

The section of this Report dedicated to foreign intelligence services will most probably become the subject of many public debates, as it always attracts the most attention from media and general public. Nevertheless, it should be noted that the BIS monitors the activity of all foreign intelligence services on Czech soil. Consequently, it can be clearly affirmed that the most active services are those of Russia and the PRC. However, the BIS also monitors the activity of other foreign intelligence services present in the Czech Republic, for example the services of Iran and North Korea.

Another important chapter of our annual reports focuses every year on the major economic interests of the Czech Republic. Same as in other sections of the Report, this chapter outlines in general terms the phenomena and areas, which the BIS assesses as important. The BIS delivered detailed information on these matters to the entitled addressees in the course of the year and summarized its findings in the classified and more extensive Report on the Activities of the Security Information Service for 2019.

Despite the general nature of the information in this Report, I believe that it provides a vivid picture of the Service's work and I hope that you will find the contents of the Annual Report for 2019 as interesting as in the past years.

Col. Ing. Michal Koudelka
Security Information Service Director General

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 the Czech law, namely in Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended, and Act No. 154/1994 Coll., 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.

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

- Schemes and activities directed against the democratic foundations, sovereignty, and territorial integrity of the Czech Republic,
- 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 Coll., the BIS also fulfils other tasks as defined by specific legislation (e.g. Act No. 412/2005 Coll., on the Protection of Classified Information and Security Eligibility, as amended) or international treaties, by which the Czech Republic is bound.

Furthermore, Section 7 of Act No. 153/1994 Coll. stipulates that the responsibility for the activities of Czech intelligence services and for the coordination of their operations 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 Government's knowledge and within the scope of the Service's powers and responsibilities.

To fulfil its tasks, the BIS is authorized to cooperate with other intelligence services of the Czech Republic. Section 9 of Act No. 153/1994 Coll. 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 Coll., the BIS may cooperate with intelligence services of foreign powers only with the consent of the Government.

2 Intelligence Activities and Findings

In 2019, the BIS paid increased attention to activities, which jeopardize the Czech Republic's security or major economic interests. This is why most of its reports focused on this domain.

Hostile activities of foreign powers also posed a great threat to the security of the Czech Republic in 2019. This is why the BIS put a considerable effort into the assessment of potentially threatening activities concerning strategic projects in the domain of energy and information and communication technologies, for example. The BIS sees potential dependence on suppliers from countries, which have long acted against the Czech Republic, its interests or its NATO and EU allies, as most undesirable for the security of the state.

In 2019, the BIS also paid considerable attention to the actions of individuals with ties to terrorist or radical groups and organisations, in order to identify and eliminate any risks or threats to the national security. Organized crime constituted another set of threats, which were however mostly connected to other security concerns, e.g. major national economic interests or hostile activities of foreign powers.

A summary of all intelligence activities, in which the BIS engaged in 2019, is part of the classified Report on the Activities of the Security Information Service for 2019 – a report the BIS submits annually to the President of the Czech Republic and the Government in accordance with Section 8, Paragraph 1 of Act No. 153/1994 Coll.

During the course of 2019, the BIS informed the entitled addressees, in accordance with Section 8 of Act No. 153/1994 Coll., about individual intelligence findings and the results of analyses, on which the overview of it activities in this public annual report is based. In 2019, the BIS submitted more than 200 documents to the President and Government Ministers. On top of that, further reports were shared with 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*), the Military Intelligence (in Czech: *Vojenské zpravodajství – VZ*) and other state authorities.

2.1 National Security and Major Economic Interests

Protection of Major Economic Interests

In 2019, the BIS paid increased attention to phenomena threatening strategic projects, whose importance for the security of the Czech Republic reached beyond the scope of the country's major economic interests. These projects concerned mainly energy and information and communication technology. As in the recent years, the BIS focused on threats in the form of interventions against the independent work of Czech national regulatory and supervisory bodies. The BIS noticed a number of cases relating to illegal lobbing, clientelism and corruption, the nature of which was similar to the previous year.

In 2019, the public administration and state-run companies started or continued the implementation of several important economic projects with a strong connection to the security interests of the state. The preparation, implementation and completion of these projects were directly

connected to security interests of the Czech Republic, i.e. to maintaining energy and cyber security or to increasing economy competitiveness[1]. Indirectly, with respect to their economic extent and measure of their impact on the strategic security interests, these projects also had influence on vital security interests[2], e.g. political independence and sovereignty of the Czech Republic.

The most substantial threat common to all monitored cases was the potential participation of problematic entities with the capability as well as motivation to abuse their position in the projects to reach their own particular interests or act in the interest of third parties, e.g. foreign powers, against the interests of the Czech Republic. Based on the nature of the projects, the threats could consist mainly of misusing access to a great volume of sensitive data (personal, economic, security) or creating dependency on supplies from unreliable suppliers, which would make the completion of the projects vulnerable to later economic, political or security demands. In such cases, the risks can also include possible dependency on the supplier after the end of the project, leading to undesirable consequences (vendor lock-in).

The problematic entities, as described above, are considered to predominantly originate from countries, where state administration has the potential to assert its foreign-political aims, irrespective of the economic interests of local companies, even if they are in private hands. Furthermore, the issue is closely connected to foreign investments regarded as a security risk and to the mechanism for the identification of investment-related security threats. The investor being from an authoritarian state is one of the important factors in the risk-level assessment of particular investments.

In general, an analogous perspective can be applied to unreliable Czech entities pursuing commercial relations with state institutions. The BIS identified cases of dubious companies (short history, missing references, connections to persons with a criminal record etc.), which have built their business and investment plans mostly on untrue or exaggerated claims of alleged support from state institutions and officials. Representatives of these companies managed to skilfully use even the most marginal meetings to collect materials for subsequent manipulative and distorted enhancement of their reputation. Consequences of such activities jeopardized the good reputation of both the individual participants and the Czech Republic.

In some sectors, especially in energy, healthcare and telecommunications industries, the BIS monitored intensive efforts of important market players to influence the legislative process and staffing or operation of regulatory bodies by illegitimate means. Usually, no illegal methods were used, although the companies pushed ahead their interests in a way which was much more aggressive than usual lobbying. The most often used means were distorting data and materials origin in order to create the semblance of objectivity, raising unfounded concerns about negative consequences for the people in charge or efforts to influence the staffing of key authorities.

A persisting phenomenon with long-term grave negative impact on economic interests of the state were cartel agreements between suppliers, who apply for contracts launched by state institutions or companies. The commissioning entities often had limited possibilities to prevent negative consequences, even if they knew about the secret agreements. It was either difficult to prove

[1] See Security Strategy of the Czech Republic 2015.

[2] Ibid.

the existence of cartel agreements or the end of cooperation with key suppliers would have had negative impact, since the cartel agreements were often related to essential state assets, e.g. strategic infrastructure.

BIS also informed on the negative impacts of continuing disadvantageous commercial relations between state institutions and private entities. The prevailing trend was that these problems concerned mostly ICT projects and government support for export business.

Furthermore, in specific cases, the BIS has documented a number of negative phenomena, which had been described already in the previous years, primarily failures caused by negligence, corruption and clientelism. As a consequence, state-owned companies had to cope with sensitive information leaks, purchases of unnecessary or overprized services and goods, high costs caused by suspended economic activity, and disadvantageous property sale and lease contracts. For example, the BIS informed on several cases of long-term relations between a private supplier and a contracting public entity, which were based primarily on personal ties between decision makers. This resulted for example in supplier's shortcomings being overlooked, sanctions not being applied or non-public information being divulged. The usual motivation of state officials was not corruption, but a tendency to make their own work easier by, for example, avoiding possible conflicts with new, unknown suppliers. When state officials were implicated in corruption, they often accepted only material benefits of rather insignificant value and completely incomparable with the scale of the contracts in question. However, the receivers were given a certain sense of exclusivity.

Proliferation of Weapons of Mass Destruction and Trade in Military Material

The BIS contributes to the Czech Republic's international commitment to fight proliferation of weapons of mass destruction (WMDs) and their carriers, i.e. chemical, biological and radiological agents, as required by International Control Regimes (ICRs)[3], United Nations Security Council (UNSC) resolutions, the Organisation for Security and Cooperation in Europe (OSCE) and EU Council's regulations, directives and common positions. In the Czech Republic, WMDs are completely excluded from trade and the sale of dual-use items is regulated by both EU[4] and national[5] legislation in order to lower the risk of their misuse in military programs of countries that pose a proliferation threat.

Apart from the above mentioned undertakings, the BIS also strives to prevent proliferation of other items as specified by international treaties and commitments. These agreements include the Arms Trade Treaty (ATT) or the Treaty on Conventional Armed Forces in Europe. As a NATO member, the Czech Republic is obligated not to export arms, military material, munition or explosives to

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

[4] Council Regulation (EC) No 428/2009, setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

[5] Act No. 594/2004 Coll., Implementing the European Community Regime for the Control of Exports of Dual-use Items and Technologies; Act No. 38/1994 Coll., on Foreign Trade with Military Material.

countries, which are subject to arms embargos or do not provide guarantees against the possible resale of these goods, or to non-state actors with ties to terrorist groups. Any breach of the Czech Republic's international commitments would have negative impact on the country's security and economic interests as well as its good reputation and international position. On top of that, the BIS aims to stop any proliferation activity, which could result in secondary issues with a direct impact on national security.

In 2019, countries of proliferation concerns, such as North Korea, Syria, Iran or Pakistan, continued their covert attempts to procure internationally controlled items. The countries used less known or purpose-created companies and third countries for re-exportation and tried to disguise money transfers in order to avoid being traced back.

The attacks on Saudi civilian infrastructure in September 2019, including oil processing facilities in Abqaiq and Khurais, are a good example of the risks posed by re-exportation and reverse engineering of controlled items. The analysis of missile debris led to the conclusion that the attackers used copies of Czech engines. These engines had been constructed using the method of reverse engineering with the use of some original parts. The investigation of the attack has not been concluded in 2019.

Another case, which was disclosed in 2019 but took place earlier, illustrates well the use of elaborate re-exportation routes. This time North Korea tried to procure tank and armoured vehicle engines from the Czech Republic. The BIS discovered that North Koreans were trying to re-export the engines through Moldova, where the cargo was re-labelled as fishing boat engines in customs declarations. The cargo was then supposed to be transported to Ukraine, where it would be re-labelled again as power generator engines. The deal was guaranteed by banking institutions form several countries. Based on the BIS intelligence, the re-exportation process was cancelled.

The BIS has gathered a considerable volume of information concerning various attempts to circumvent international sanctions by Iran, Russia, and a number of states in the Middle East, South East Asia, Caucasus and Africa. The BIS also informed on other states, such as the People's Republic of China (PRC), Russia or other countries governed by unstable and repressive regimes as well as countries troubled by armed conflicts, have tried to procure military material, arms, explosives or components for the development and production of e.g. unmanned aircrafts (drones).

2.2 Intelligence Services and Hostile Activities of Foreign Powers

Within its scope of powers and responsibilities, the BIS inquired into the activity of all intelligence services operating on the Czech territory against the interests of the Czech Republic in 2019. Given the priorities set by the Government, the level of threat posed to the interests of the Czech Republic, and the available resources, the BIS's intelligence work in 2019 focused mainly on the activities of Russian and Chinese state-controlled structures, which put the security and other key interests of the Czech Republic at risk.

Although Russia uses more and more often unconventional concepts when pursuing its interests, Russian intelligence services still play an important part in the country's actions and operations. Russian intelligence officers can be identified as – or at least appear to be – those, who supervise and control hostile activities, even when these activities are conducted by non-state entities.

The intensity of Chinese intelligence and influence activities does not fall behind the Russian ones. However, there is an important difference: while Russia tries to destabilize and overthrow its rivals, the PRC wants to establish a global sinocentric community, in order to make other countries recognize the legitimacy of Chinese interests and show respect, which the PRC believes it is entitled to.

The Czech Republic has also been the target of cyber activities of Russian and Chinese state-linked actors. In 2019, the BIS registered further security incidents linked to the operations of cyberespionage groups supported or directed by foreign governments, such as Turla, Zebrocy, APT28 or APT15.

On top of that, some activities and interests of the Vietnamese government in the Czech Republic were to some extent also identified as a threat. As part of its anti-terrorism efforts, the BIS also monitored Iranian intelligence services.

Russian Intelligence Services

In 2019, officers and agents of all Russian intelligence services were active and conducted intelligence activity in the Czech Republic: Foreign Intelligence Service (SVR), Foreign Military Intelligence (GRU), Federal Security Service (FSB), and Federal Protective Service (FSO).

It is no surprise that the activities of Russian intelligence officers, who use the Russian diplomatic mission in the Czech Republic as their cover, were mostly meant to help Russian foreign-political interests, improve Russia's image and promote Kremlin's policies. For a few years, there has been no significant change in the number of Russian intelligence officers operating under diplomatic cover in the Czech Republic. However, reducing their activity effectively was still extremely complicated, as the Russian diplomatic mission has been disproportionately large in comparison to the Czech mission in Russia for a long time.

In the previous years, the BIS has been monitoring the efforts of the Russian Foreign Ministry and the SVR to gain control over the Russian-speaking community in the Czech Republic, primarily by supporting a part of the community, which sympathizes with the Kremlin. In 2019, the Russian state toned down these activities and according to available intelligence, it did not even direct in the well-publicized vitriolic campaign led by pro-Kremlin members of the Russian diaspora against the Russian representative in the Government Council for National Minorities.

The transition from state-controlled or directed activities to spontaneous actions fits the pattern of Russian unconventional coercive methods. When Russian state officials express what they desire to happen (for instance by spreading manipulative information), proxy actors without any links to the Russian state proceed to action on their own initiative and based on what they think the officials might want. In this kind of situation, the key psychological element is that proxy actors are convinced they have "the duty to act".

The possibility that a foreign power does not engage in any direct action and keeps its distance, while using various ways (PR, instigating statements, propaganda etc.) to inspire individual persons to take action, is considered by the BIS as a threat. This threat would become even more serious, if the number of individuals susceptible to the instigations were to rise in the future, regardless of whether these individuals would be members of the Russian-speaking community or Czech nationals.

Chinese Intelligence Services

During 2019, the most active Chinese intelligence services in the Czech Republic were the Ministry of State Security (MSS) and the Military Intelligence Department (MID). Representatives of the International Liaison Department of the Central Committee of the Communist Party of China (ILD) in the Czech Republic established official relations, but also used methods of intelligence work, when pursuing their goals.

Chinese intelligence officers used traditional covers, posing as diplomats, journalists or scholars, as well as modern methods of intelligence work (e.g. social media). The intelligence services focused on a number of areas of interest and took advantage of the fact that Czech businesses are welcoming towards Chinese investors. Their areas of interest included technology, the military sector, security, infrastructure projects, healthcare, economy, environment, and both foreign and domestic policy.

Chinese entities in the Czech Republic – intelligence officers, diplomats, party officials etc. – sought to find ways to influence public opinion, spread propaganda and present a positive image of the PRC, using both overt and covert influencing of Czech media.

Positive articles about the PRC were supposed to build a pro-Chinese environment and create new opportunities for Chinese expansion. The articles were also meant to make an impression on Chinese readers, when they reappeared later in Chinese press, which presented them as the opinion of Czech mainstream media or even as the opinion of the whole Czech Republic. Often, the cooperation between Czech and Chinese media has been taken care of by the PRC's intelligence services. The Czech media thus became an instrument of Chinese intelligence services in projecting Chinese influence.

The PRC's intelligence services took considerable interest in the Czech academia in 2019. The increasing cooperation between the Chinese and Czech universities included new programs for the exchange of students and researchers, for launching joint research centres and for research cooperation etc. Czech academics received numerous invitations to seminars, conferences and meetings in the PRC, which were all paid for by the Chinese hosts. Given that the Chinese intelligence services prefer to make contact on Chinese soil or in a third country (i.e. never in the person of interest's country of origin), these events can become an opportunity to approach targeted persons. Even if they make no contact, the PRC can use the participation of researchers in various cooperation platforms in its propaganda or at least make use of the sense of obligation stemming from Chinese hospitality.

Generally, the academia is a sensitive community, which can be easily approached by intelligence services as well as other influence actors due to its openness. Given the nature of the PRC's regime and legislation, it is often difficult to distinguish between independent academic research and state interests. This is why it is difficult to identify the PRC's intelligence officers or individuals acting in favour of Chinese intelligence services, who use academic cover, also considering that researchers with links to Chinese intelligence services are often senior scholars working with renowned institutions. Generally speaking, researchers suspected of or identified as working for the Chinese intelligence services tend to extend the scope of their research to gathering information on the PRC's areas of interests, i.e. domestic and foreign policy, defence and security forces, technology, industry, infrastructure and energy projects etc.

Russian and Chinese Cyberespionage Activities

In 2019, the BIS continued its investigation into the attack, which had compromised the unclassified network of the Ministry of Foreign Affairs and had been perpetrated by a group in the service of a foreign power, most probably Russia.

Later it became clear that the Ministry's network had been also compromised by another malware, which has been attributed to a cyberespionage group of a different foreign state actor.

Czech diplomatic missions also became the target of cyberattacks by foreign state actors. In 2019, two cases of compromised networks were identified.

Apart from the above-mentioned incidents, the BIS also took part in the second half of the year in the investigation into the attack on the ICT infrastructure at one of the Czech diplomatic missions to international organisations. In late 2018, at least one device had been compromised during an intensive global cyberespionage campaign led by a foreign state actor, most probably Russia. Hackers accessed the device, when a user opened a text file attached to a phishing email. Detailed analysis discovered that the device in question had been also infected in past years with malware attributed to a cyberespionage group linked to another state actor.

In September 2019, the BIS received information that a probably Chinese cyberespionage group had penetrated the infrastructure of the cybersecurity company Avast. After being notified by the BIS, the company launched an extensive audit of its internal network and discovered it had been compromised on a serious level. The cooperation with the BIS allowed Avast to adopt considerable security measures and ultimately contributed to the protection of user data.

State actors that attack not only Czech targets most often used phishing/spear-phishing emails containing compromised attachments (e.g. macro-enabled files) as their attack method. This way, hackers attempted to install malware onto devices without much help from users. In one case, hackers tried to make the recipient download malware from a hidden link in the body of the phishing email.

2.3 Protection of Constitutionality and Democratic Foundations

Disinformation and manipulative media reports continued to spread throughout 2019. It resulted in increased polarization of the society, less faith in the democratic rule of law and its institutions, and growing support of foreign interests. In the last few years, we have seen the formation of a rather solid disinformation scene composed of media, which present themselves as independent or alternative sources of information. More and more often, these media are trying to get rid of the disinformation label and make attempts to gain legitimacy in mainstream media. Such activities can been seen as part of a larger phenomenon, i.e. conspiracy theories, pro-Russian narratives and anti-Western views being wilfully shifted from peripheral into mainstream media.

Prior to the European Parliament elections in May 2019, the BIS monitored possible illegitimate attempts to influence the result of the elections. Although there has been a visible increase in reporting containing biased narratives (mostly anti-EU, anti-immigration or pro-Russian), the BIS did not find any indication that the election process might have been compromised by either domestic or foreign actors.

Traditional extremist groups did not find any issues in 2019, which would allow them to mobilise their supporters or the general public. Left-wing and right-wing extremists therefore did not gain enough momentum to pose a threat to the safeguarding of the constitutionality of the Czech Republic. The same applies to existing paramilitary groups.

Pro-Russian Activism

Pro-Russian activists, i.e. persons sympathizing with Russia, who wittingly or unwittingly act in direct support of foreign interests, continued in the same activities in general as in 2018. The activists kept expressing strong and systematic criticism of the current political order of the Czech Republic and its membership in the EU and NATO. The majority of issues they have focused on corresponded to the priorities of the Russian government.

In the second half of 2019, Kremlin supporters focused on fighting against the memorial of Soviet Marshal I. S. Konev being removed, as decided by the municipal council of one of Prague's districts. First, the memorial had been covered, which provoked criticism towards the municipality by the Russian embassy. A wide spectrum of activists then took part in protests against the memorial's removal, using the opportunity for their self-promotion.

As in the previous years, subversive activities against Ukraine directed by Russia also took place in 2019.

Paramilitary and Militia Groups

The nature of activities of paramilitary and militia groups has not changed significantly in 2019 and that is why they did not constitute an actual threat to national security. This was the result primarily of the dismal state the groups were in because some of their leaders had left them.

The most significant mobilization topic for the otherwise passive militia scene became the plan of the Ministry of the Interior to outlaw the creation of armed paramilitary groups. The plan for the legislative change stirred the leaders of the main countrywide organisations into more action and by the end of 2019, they have developed stronger cooperation. As a result, paramilitary and militia organisations can be expected to transform themselves in order to avoid financial or other repercussions. For example, the groups could redirect their activity towards defence education and training.

Traditional Political Extremism

Traditional left-wing and right-wing extremist groups have been in decline for several years. Remaining groups are splintering and weakened by ideological fragmentation and numerous personal conflicts. As a result, they are unable to attract new members and sympathizers. One of the reasons, why there has been less and less activity among extremists, is that extremist groups have difficulties finding a cause, which would allow them to mobilize the extremist scene and its supporters.

One of the reasons for this is a gradual shift in public debate and an increased public tolerance to hate speech that allowed other political entities to take control of issues used by extremists in the past.

The only notable event, which resulted in renewed activity of traditional extremists, was the removal of Marshal Konev's memorial in Prague. At this occasion, Marxist-Leninist extremists joined pro-Russian activists and disinformation propagators during the protests.

2.4 Terrorism

The situation related to terrorism and Islamist radicalization remained calm in the Czech Republic in 2019 and the BIS did not document any indication of the Czech territory being used as either logistic or ideological base by the supporters of international Islamist terrorism. In connection with the latest development outside the Czech Republic and the ever more important need to identify lone, self-radicalised individuals in a timely manner, the BIS has conducted an increased number of background checks on individuals, who were assessed as susceptible to potential involvement in terrorism.

Main factors, which could lead to radicalisation of the Czech Muslim community, were the same as in the previous years. These factors included namely ideological propaganda spreading from abroad (and occasionally from the local community), Islamophobic opinions persisting in part of the Czech society, and events in foreign countries related to the Muslim world.

The Christchurch terrorist attack in New Zealand in March 2019 is a good example of how this type of events can lead to radicalisation in other countries. In reaction to the attack, Leonid Kushnarenko, chairman of the Muslim Community of Prague, encouraged Czech Muslims to buy arms. However, Kushnarenko's statements provoked negative reactions regarding not only him but also the whole Czech Muslim community. The Czech Muslim organisations therefore forced Kushnarenko to resign his positions.

The BIS also monitored the impact of events in the Middle East and other conflict zones on the situation in the Czech Republic. One such event with international fallout was the Turkish offensive in Northern Syria. However, the offensive did not provoke any unrest or conflict in the community. There has been also no conflict between local Kurds and Turks either. The relation between the two communities has been for a long time based on shared business activities.

In 2019, the BIS received information on the death of one of the fighters, who volunteered to join armed groups in the Middle East in the years between 2012 and 2017. If this is true, he would be the fifth dead fighter, who had left Czech Republic. Two more fighters were supposed to be still in Syria, while there has been no new information regarding the others. Possible return of these individuals is a permanent risk, as it could lead to the radicalisation of the Czech Muslim community. However, in 2019, the BIS has received no new information on fighters returning from abroad to the Czech Republic and according to available information, no more persons left the country for conflict zones.

In comparison to 2018, the BIS has registered fewer open manifestations of support to the so-called Islamic state (ISIS) among Sunni Muslims, since the Islamist caliphate lost both its territory and appeal. Nevertheless, there have been some individuals constituting a security risk, as they continued

to express negative attitudes towards the Czech society. The reasons why they adopted radical views were mainly insufficient integration, loss of family ties, financial difficulties, criminal behaviour and drug use. The BIS focused on finding individuals, who have recently turned towards the Islamic religion, while also showing signs of the above-mentioned behaviours and risks. No individuals were identified as a risk to national security in 2019.

As in the previous years, the BIS continued to investigate signs of possible Islamist radicalisation and monitored these activities also on the Internet with special attention on social media. Internet and social media users, whose posts in Internet discussion contained views based on radical religious ideology, did not constitute a security threat in general. Their radical behaviour was most often a form of attention seeking among the Internet community or it was the result of a psychological disorder. The BIS regularly cooperated with the Czech Police National Centre for Combating Organised Crime (*in Czech: Národní centrála proti organizovanému zločinu – NCOZ*), when identifying and assessing the risk level of individual authors of radical emails and posts on social media.

In 2019, the medical aid programme for Libyans, which brings dozens or even hundreds of Libyan patients to Czech spas and rehabilitation facilities every year, was still in place. Most of the patients come to the Czech Republic within the framework of the so-called military veteran aid programme, which is completely financed by the Libyan government. Bearing in mind the security risks of the programme, preventive measures have already been taken in cooperation with other government bodies, in order to detect any individuals among the patients and those accompanying them, who might become a threat to national security. Despite the adopted precautions, there has still been the risk that the medical aid programme could be exploited for other purposes or that it could even permit Islamist radicals to enter the Czech territory.

The BIS continued to monitor the Kazakh “Pure Islam” sect, whose members still isolate themselves from the majority of the society, create closed communities and refuse integration. This particular form of Islamism is followed in the Czech Republic by several dozens of families, who have various forms of residence status and ties to similar communities abroad.

Given that Iranian government continues to support terrorism in the world, the BIS also paid attention to the activity of Iranian intelligence services, which have conducted their actions on European soil with growing aggressiveness in the recent years. In 2018, the Iranian intelligence service MOIS was preparing a bomb attack on a conference in France organised by an Iranian opposition group, the Mujahedin-e Khalq. The head of the attackers was an Iranian diplomat posted in Austria. In 2019, the BIS lead an investigation into the earlier visits of this Iranian national to the Czech Republic.

As part of its powers and responsibilities, the BIS contributed to the inquiries into terrorist incidents across Europe, which took place in 2019. The information it obtained was shared with the Service’s concerned foreign partners.

3 Protection of Classified Information

3.1 Administrative Security

The year 2019 brought no significant changes to the domain of protection of classified information. Similar to 2018, the BIS drew up expert opinions and assessed the classification of documents in accordance with Act No. 412/2005 Coll. Within its sphere of powers, the BIS also provided interpretation of the list of classified information and related internal regulations and provided methodical support to the Service's sub-units.

3.2 Security of Information and Communication Systems

The security supervision of the Service's information and communication systems is regulated by the BIS ICT Security Policy. The aim is to provide high level of information security and increase trust in the security of information systems. The BIS focuses on continuously improving the security of ICT systems and services provided – in classified as well as unclassified systems. The ICT systems are protected from both outside and inside misuse.

All classified information systems within the BIS are certified by the National Cyber and Information Security Agency (in Czech: *Národní úřad pro kybernetickou bezpečnost - NÚKIB*). In 2019, security documentation has been updated and the information system for processing information classified as Top Secret was successfully re-certified.

All users of certified information systems are trained in accordance with Act No. 412/2005 Coll. before accessing the systems for the first time and then undergo annual trainings. The training focuses on cyber security, too.

In 2019, the BIS detected no serious incidents which could have compromised the functioning of the information and communication systems or cryptographic devices. Cryptographic material was regularly inspected and no shortcomings in management and manipulation have been detected.

3.3 Physical Security

In the domain of physical security, the BIS continued to improve security mechanisms and systems used to protect the Service's facilities in order to ensure the security of classified information in accordance with Act No. 412/2005 Coll. and Regulation No. 528/2005 Coll. on Physical Security and Certification of Technical Means, as amended.

Physical security related policies have been updated to reflect the current situation and further documentation on the Service's facilities has been created.

3.4 Crisis Management

For the purposes of protection of classified information in emergencies, Building and Area Security Plans and emergency plans have been updated.

4 Cooperation with Czech Intelligence Services 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. Further cooperation with these services takes place at different levels encompassing operational, analytical and technical issues as well.

Close cooperation with the Office for Foreign Relations and Information and with the Military Intelligence focused on the fight against hostile activities of foreign powers, cyber security, terrorism, proliferation of WMDs and their carriers, and on illegal trade in military material.

4.2 Cooperation with the Police of the Czech Republic

The BIS provides information to the President, the Prime Minister, and other Cabinet Ministers and under Section 8, Paragraph 3 of Act No. 153/1994 Coll., the BIS also provides information to the Police of the Czech Republic, if this does not jeopardize an important intelligence interest. In many cases, cooperation between various departments of the BIS and the Police draws on the nature of submitted information. Information is also provided upon requests by the Police or public prosecutor's office, pertaining to specific criminal proceedings.

The BIS continued its cooperation with various Police departments, namely with the Directorate of the Alien and Border Police (in Czech: *Ředitelství služby cizinecké policie – ŘSCP*) in the security risk assessment process regarding visa applications. Since 2000, the BIS contributes to the security assessment by guaranteeing the common position of the Czech intelligence services. In 2019, the BIS provided assessment of nearly two million applications for short-term Schengen visa, which had been submitted at an embassy of the Czech Republic or another Schengen Area country, which then requested cooperation of the Czech authorities.

Another form of cooperation between the BIS and the Police are credibility assessments of natural persons in relation to the 2015 amendment of Act No. 49/1997 Coll., on Civil Aviation, which stipulates provisions regarding reliability certificates issued to natural persons by the Civil Aviation Authority (in Czech: *Úřad pro civilní letectví - ÚCL*). These screenings include background checks on natural persons conducted by the Police. Based on the Police's requests for cooperation on assessing credibility of natural persons, the BIS provided assessments of more than 8 000 individual applicants for the ÚCL certificate.

In 2019, the cooperation with the Police National Centre for Combating Organised Crime took the form of exchange of intelligence on major economic interests, terrorism and the protection of constitutionality and democratic foundations of the state. The cooperation mostly concerned security screening of entities of interest. Findings in the area of economic crime and cyber security were shared as well.

In the domain of physical security, the BIS cooperates with the Police of the Czech Republic on security protection of the BIS buildings.

4.3 Cooperation with other State Authorities and Institutions

Close cooperation of the BIS and the National Security Authority (in Czech: *Národní bezpečnostní úřad – NBÚ*) on protecting classified information continued. The cooperation involved mainly investigations based on the National Security Authority's requests. The BIS conducted investigations regarding personnel and industrial security, security clearance background checks, and inquiries in order to determine whether natural and legal persons holding security eligibility certificates still meet all legal requirements. Throughout the year, meetings regarding the cooperation on specific issues were held.

Fulfilling its obligations under Act No. 412/2005 Coll., the BIS was asked by the National Security Authority to conduct more than 20 000 security clearance investigations for the issuance of security clearance certificates for natural and legal persons.

In addition to its work on the National Security Authority's 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 National Security Authority, or if the information concerns employees or officials of intelligence services, to the services concerned. The BIS also routinely shares information in reaction to numerous and repeated National Security Authority's requests for possible information on holders of security clearance or security eligibility certificates (requests pursuant to Section 107, Paragraph 1, Section 108, Paragraph 1, and Section 109, Paragraph 1 of Act No. 412/2005 Coll.).

Regarding the fight against terrorism in 2019, the BIS took active part in the regular meetings of the working platform, which collects, processes and shares information on risk individuals suspected of activities related to terrorism. The platform called the National Contact Point for Terrorism (in Czech: *Národní kontaktní bod pro terorismus – NKBT*) falls under the National Centre for Combating Organised Crime of the Czech Police. National Centre for Combating Organised Crime, the BIS, the Office for Foreign Relations and Information and the Military Intelligence are partners within the National Contact Point for Terrorism. In the first half of 2019, the Financial Analytical Office (in Czech: *Finanční analytický úřad – FAÚ*) became part of the platform. It participates in the exchange of information with aim to fight against terrorism financing. The BIS also played an active role in the Joint Intelligence Group (in Czech: *Společná zpravodajská skupina*), the permanent working body of the Government's Committee for Intelligence Activity (in Czech: *Výbor pro zpravodajskou činnost*), the target of which is intelligence exchange and coordination between Czech intelligence services, the Police, the Ministry of the Interior and the Ministry of Foreign Affairs. The Group is meant to identify security threats that the Czech Republic is facing, particularly in the area of terrorism.

The BIS cooperated also on projects of other state authorities (e.g. the Ministry of the Interior and the 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 received and processed requests of other state authorities that pertained to more than 160 000 natural and more than 700 legal persons in total. In this respect, there was an extensive cooperation with the Ministry of the Interior concerning the assessment of foreigners applying for international protection, residence permits or Czech citizenship. The cooperation also concerned vetting of legal and natural persons applying for permits for employment facilitation services. Within the interdepartmental cooperation with the

Ministry of Foreign Affairs, the BIS provided its assessment of persons seeking to collaborate with the Ministry of Foreign Affairs, of interns and employees at Czech Embassies, journalists seeking accreditation, or honorary consul nominees.

BIS representatives took part in the meetings of the National Security Council's (in Czech: *Bezpečnostní rada státu*) working bodies – Committee for Intelligence Activity, Committee for Cyber Security, Committee for Domestic Security, Committee for Coordination of Foreign Security Policy, Committee for Defence Planning and Committee for Civil Emergency Planning. Expert departments of the BIS drew up opinions and comments on materials of the National Security Council and its Committees.

Active cooperation was also conducted within the Interagency Body for the Fight against Illegal Employment of Foreigners or the working group of the Permanent Committee on Nuclear Energy focused on state security interests in the area of nuclear energy.

In 2019, the BIS also cooperated intensively with the National Cyber and Information Security Agency, General Inspection of Security Forces (in Czech: *Generální inspekce bezpečnostních sborů – GIBS*), Financial Analytical Office, Customs Administration (in Czech: *Celní správa ČR*), General Directorate of Customs (in Czech: *Generální ředitelství cel – GŘC*), Prison Service (in Czech: *Vězeňská služba ČR*), General Financial Directorate (in Czech: *Generální finanční ředitelství*), courts, and public prosecutors.

Cooperation with other national administration bodies also pertained to specific cases of proliferation of WMDs and their carriers and trade in military material. Cooperation was conducted primarily with customs administration bodies both on the level of the General Directorate of Customs and individuals customs directorates. The BIS continued its cooperation with customs administration bodies in order to prevent potential export of controlled items, i.e. primarily military material and dual-use items, to sanctioned countries. In specific cases, the Service cooperated with the Ministry of the Interior, Ministry of Defence, Ministry of Foreign Affairs, Licensing Administration of the Ministry of Industry and Trade, State Office for Nuclear Safety (in Czech: *Státní úřad pro jadernou bezpečnost – SÚJB*) and their subordinate organizations, with aim to contribute to authorization and licensing proceedings and to provide information on the compliance with license conditions and requirements of international control regimes.

In addition to providing and exchanging information, the BIS gives other state authorities generalized findings and recommendations regarding various legislative and non-legislative documents. Furthermore, the BIS provides various training courses, consultancy cooperation, etc.

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. As far as multilateral cooperation is concerned, the BIS was active in several organizations, e.g. the Counter-Terrorist Group or NATO Civilian Intelligence Committee.

The BIS received more than 10 000 reports from its foreign partners and sent almost 2 000 documents. BIS representatives took part in more than 800 international strategic and expert meetings.

The level of international information exchange was similar to the previous year. The cooperation in 2019 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 countries.

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, Paragraph 1 of this Act stipulates that the activities of intelligence services are subject to oversight by the Government, Parliament and 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 in relation to the Inspection Code that is defined in Act No. 255/2012 Coll., the Inspection Code.

Act No. 153/1994 Coll. defines neither the scope nor the manner of Government oversight. The Government's oversight powers are based on its entitlement to assign tasks to the BIS within the Service's legal powers and responsibilities and to assess their fulfilment; 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. This shows that Government oversight focuses on all activities of the Service.

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, i.e. its respective body for intelligence services, is informed about the activities of Czech intelligence services by the Government. Direct parliamentary oversight of intelligence services as stipulated by Section 12 of Act No. 153/1994 Coll. is defined by special legislation; therefore, the above-mentioned respective body for intelligence services assumes to a certain extent the role of parliamentary oversight of the Government. Since January 1, 2018, the purview of the respective body has been assigned to special bodies for the oversight of intelligence services. For BIS, this authority is a special oversight body established in accordance with Act No. 154/1994 Coll., on the Security Information Service, as amended (please see below).

The special legislation mentioned in Section 12, Paragraph 1 of Act No. 153/1994 Coll. is Act No. 154/1994 Coll., on the Security Information Service, as amended. Under Section 18 of 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 Act No. 154/1994 Coll. provide specifically for the particular powers of the Oversight Commission. Authorized members of the oversight body may, e.g., enter the Service's buildings when accompanied by the BIS Director or by a BIS official designated by the Director for this purpose; or request due explanation from the BIS Director should they feel that the activities of the BIS illegally violate the rights and freedoms of the Czech citizens. The Director of the BIS is obliged to provide legally defined information and documents to the Oversight Commission.

Legal regulations pertaining to the oversight of intelligence services underwent a significant change by the adoption of Act No. 325/2017 Coll., amending Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended, and other relevant acts. Act No. 325/2017 Coll. came into force on January 1, 2018.

According to this new legal regulation, a five-member expert oversight body, the Independent Authority for the Oversight of Intelligence Services of the Czech Republic, should be newly established. Members should be elected by the Chamber of Deputies for five years based on a Government proposal. The Authority should perform oversight on the basis of an incentive from one of the special oversight bodies (this amendment newly establishes the special oversight body for the Office for Foreign Relations and Information as well). The Independent Authority for the Oversight of Intelligence Services of the Czech Republic should be entitled to require from an intelligence service all necessary information on its operation that has to do with the performance of oversight. There is an exception for information that could disrupt an ongoing operation, identify members of the intelligence service conducting intelligence activity, identify persons acting in favour of the intelligence service, endanger other individuals, whose safety constitutes a major interest of the intelligence service, or violate requirements of a foreign intelligence service regarding confidential information not being provided to a third party. This Authority has not been established yet.

Oversight regarding the Service's 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, and in Act No. 166/1993 Coll., on the Supreme Audit Office, as amended.

Section 13a of Act No. 153/1994 Coll. stipulates other types of oversight activities and its aim is to protect the classification of the operation of intelligence services. Oversight activities in the facilities of the intelligence service can be undertaken only if approved by the Director of the intelligence service in question. If the approval is not granted, the intelligence service will arrange for such oversight activities within its scope of powers and responsibilities and will submit a report on such activities to the oversight body, which had requested the approval. The report is submitted in sixty days after denying approval, unless the oversight body stipulates a longer period. The Act also stipulates that if the intelligence service is not able to arrange for such oversight activities within the scope of its powers and responsibilities, it is obliged to allow for their execution by the oversight body. The service may require special conditions related to the oversight proceedings.

The Service's operations are also subject to judicial oversight of the use of intelligence technology in accordance with Act No. 154/1994 Coll. Its Section 9 and following stipulate that the Chairman of the Panel of Judges of the High Court in Prague rules on requests for warrants permitting the use of intelligence technology and supervises the process of its use. Section 11a of Act No. 153/1994 Coll. stipulates that the Chairman of the Panel of Judges of the High Court in Prague rules on the Service's requests for reports from banks, including foreign banks, and savings and credit cooperatives on matters related to their clients and subject to bank secret.

The Court not only issues warrants based on a written request submitted by the BIS, but also supervises, whether the reasons for the request remain. If not, the Court cancels the warrant.

The public does not have any specific oversight powers, but this type of oversight nevertheless forms an important element of the general oversight of the BIS operation. The public usually conducts indirect oversight via mass media or the BIS website, where annual reports or various other announcements are available.

6.1 External Oversight

Authorities and institutions with the legal right to oversee individual activities of the BIS carry out external oversight of the Service. In 2019, three external audits were conducted. First, the national health insurance company VZP reviewed payments and regulation compliance regarding healthcare insurance coverage. The second audit focused on food safety and hygiene, i.e. safety measures and compliance with Act No. 258/2000 Coll., on Protection of Public Health, and Government Regulation No. 361/2007 Coll., on the Conditions of Occupational Health Protection and other related legislation. The review was conducted by the Health Department of the Ministry of the Interior. The third audit was conducted by the Social Security Department of the Ministry of the Interior and concerned compliance with requirements regarding retirement insurance of the BIS's personnel.

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, as amended. Its scope of powers and responsibilities is set by the organizational structure and internal regulation by the Director of the BIS. In 2019, the internal audit service completed four audits.

Other BIS expert units conducted thirty-two inspections. Their aim was to methodically and factually guide the operation of organisational units in the financial and material area, supervise the compliance with the 3E principle and prevent potential emergence of undesired phenomena. Expert and consulting assistance was part of the inspections as well.

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

Employees of the archive and of the control group carried out forty-five 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 the Service's individual divisions and documentation stored in the registry was regularly inspected.

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 misdemeanour 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.

In the area of investigation of conduct suspected of having the traits of misdemeanour or disciplinary infraction, the BIS Inspection Department focuses primarily on traffic offences on public roads, which belong to the scope of action of the Police. The Inspection Department is responsible for findings that cannot be provided by the Police but are important for the decision on the matter. Furthermore, this category includes investigation of matters related to the protection of classified information, theft of service IDs, incidents related to the health of BIS officials and conduct suspected of disciplinary infraction or of having traits of a misdemeanour.

Cases of conduct suspected of disciplinary infraction or of having traits of a misdemeanour by a BIS official were referred to a disciplinary proceeding in accordance with Chapter IV (Section 186–189) of Act 361/2003 Coll., on Service Contract, as amended.

Complaints, notifications and suggestions that the BIS Inspection Department investigated in 2019 were submitted mostly by external entities. Since 2017, the number of investigated notifications and suggestions continues to increase. In terms of content, reports made by citizens reflect society-wide developments in the Czech Republic and abroad.

The BIS Inspection Department cooperates with other state administration authorities and the cooperation primarily has the form of requests sent usually by Police departments, which are a part of criminal or misdemeanour proceedings. The number of processed requests corresponds to the long-term situation.

8 Budget

The budget of the BIS was stipulated by Act No. 336/2018 Coll., on the State Budget of the Czech Republic for 2019.

As in the previous years, salaries and equipment payments traditionally accounted for the majority of total expenditures. Payroll expenses also include severance benefits, i.e. mandatory payments to retired personnel. On top of that, new personnel receives recruitment bonuses.

Further regular expenditures were comprised mainly of spending on communication equipment and special equipment necessary for the operation of an intelligence service. Funds were also allocated for field intelligence activity. Furthermore, a significant part of the Service's budget has been allocated to outsourced services, fuels and electricity, all of which are indispensable for the functioning of the Service. Maintenance expenditures allowed the BIS to ensure proper technical condition of its facilities and other property.

A significant part of the Service's funds was invested in construction. Another important investment has been allocated to information and communication technologies. The aim was to provide the necessary server capacity and adequate communication technology solutions as well as advanced software tools, which would allow better processing, storage and analysis of information. Further expenditures were made in order to improve the security of intelligence work and data. A significant amount of funds has been used for the continual renewal of the Service's vehicle fleet.

The budget also reflects every year the requirements on the protection of classified information provided for in Act No. 412/2005 Coll. and in implementing regulations, especially in the domains of physical, administrative and personnel security, and in the domain of security of information and communication systems. The need to consider these matters in the whole spectrum of BIS activities leads to many expenditures, which are absent or very limited in other organizational units of the state.

The funds allocated to the BIS allowed all basic operational and development requirements to be fully covered. The budget also provided for crucial development of intelligence technology and information and communication technologies. Construction and maintenance expenses were also covered.

A detailed report on BIS economic management structure in 2019 in accordance with the relevant regulations of the Ministry of Finance of the Czech Republic is submitted as expenditure account of the section to the Ministry of Finance and to the Security Committee of the Chamber of Deputies of the Czech Parliament.

Indicators of Budget Section 305 - Security Information Service in 2019 (CZK thousands)

	Approved budget	Amended budget	Real data
Total revenues	160 000	160 000	247 773
Total expenditures	2 076 974	2 071 232	2 029 211