Annual Report of the Security Information Service for 2018

Table of Contents:

Reflections by the Director General of the Security Information Service

Ladies and Gentlemen,

It is my honour and pleasure to present you after a year a new public Annual Report of the Security Information Service (BIS) for 2018. I would like to start by reminding the public character of this report. Those interested in intelligence services know that the primary product of this kind prepared by the BIS each year, in accordance with the law, is the classified Annual Report intended only for entitled addressees. The classified Report is a well-arranged assemblage of the most important information on the Service´s activities over the given period. It contains a much more detailed and specific description of certain events, phenomena and analyses and at the same time shows an overview of the main information handed by the BIS to e.g. the President of the Czech Republic, the Prime Minister, ministers or other security forces during the previous year.

The unclassified and therefore public Annual Report does not and cannot provide concrete information. However, just as my predecessors, I believe that this document is important and very beneficial product giving the impartial image of the Intelligence Service. A reader will get a very clear picture of the Service´s activities, its scope of powers and responsibilities, priorities approved by the Government and, generally said, the topics and threats the BIS warned the recipients of the intelligence about.

Annual reports are part of communication with the public, i.e. with you, citizens, who have unquestionable right to know why it is important for the State to have intelligence services and, in general terms, what activities they perform for the State, for you. It is a tool of trust without which no intelligence service can fully operate in today´s global security situation.

Intelligence services have still been called secret services. However, for a long time, it has not meant they have been the organizations, whose existence has been disavowed by their governments. Nowadays, intelligence services have their own legislation, oversight authorities and also chapters in state budget, the budget we all contribute to. Everybody wants to know where his/her money goes and what it is spent for. We see restrained communication including public Annual Reports as a tool providing such information to our citizens.

No doubt there will appear critical voices calling this Report useless and telling nothing. However, every year´s huge interest in it says something different. I let everybody assess the following pages for himself/herself.

I wish you interesting reading.

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 relevant legislation, especially in Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended, and in 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.

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 the scope of 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 Finding

Primarily hostile activities of foreign powers posed a significant threat to the security of the Czech Republic in 2018. By utilizing a wide range of methods and activities, state, non-state, foreign and domestic actors tried to weaken Czech state institutions, influence official state positions related to international security and paint natural attributes of a democratic system as its weaknesses. The danger posed by these so-called hybrid threats pertained to several areas within the purview of the BIS.

Hybrid threats utilize multi-vector instruments and combine coordinated and naturally generated activity. By using economic, political, military and information pressure, they exploit seeming imperfections of state institutions and democratic processes (long legislative process, Parliament discussion, administrative procedures, etc.). The aim is to influence the decision-making process on various levels of public administration to their own strategic benefit by activity, inactivity or paralysis of the entity that is responsible for the decision-making.

The importance of cyberspace continued to grow. It has been confirmed that cybersecurity constitutes an integral part of security and that protection from unwanted activities in cyberspace forms an important element in the complex care of protected interests of the Czech Republic. Developments in cyberspace were reflected substantially in the intelligence situation in all areas of the BIS purview. This is mainly evidenced by the fact that the Czech Republic and its institutions became targets of several cyberespionage campaigns directed or supported by a foreign state power.

A summary of all the intelligence activities, in which the BIS engaged in 2018, is part of the classified *Report on the Activities of the Security Information Service for 2018* – 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 Coll.

During the course of 2018, in accordance with Section 8 of Act No. 153/1994 Coll., 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 2018, the BIS submitted almost 400 documents to the President and Cabinet members. Further hundreds of documents were sent to 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 Intelligence Services and Hostile Activities of Foreign Powers

In 2018 the BIS, within its scope of powers and responsibilities, dealt with all intelligence services operating in our territory against the interests of the Czech Republic.

In accordance with the priorities set by the Government, the threat level posed to the interests of the Czech Republic and the capabilities of the BIS, the main objectives of intelligence work in 2018 were activities of Russian and Chinese state structures threatening the security and other key interests of the Czech Republic. Russian and Chinese intelligence activities pertained to politics, diplomacy, espionage, economy and information warfare.

In Russia's case, the main threat are not elements of intelligence or para-intelligence activities, but the unconventional (so-called hybrid) character of Russian operations that are aimed at the enemy Russia perceives as the main military threat to its security: NATO and its member states, i.e. the Czech Republic as well. In Russia's case, intelligence and non-intelligence entities can exchange roles and functions, and so any authority (or its subordinate agency) can be used for intelligence operations or for their cover. The key Russian goal is to manipulate decision-making processes and the individuals responsible for the decision-making in order to force the counterparty to conduct activities to weaken itself.

The complexity of Chinese activities is comparable to Russian ones. However, given the geographic distance and the absence of historical Chinese military engagement in Europe, the BIS considers primarily the increase in the activities of Chinese intelligence officers as the fundamental security problem. These activities can be clearly assessed as searching for and contacting potential cooperators and agents among Czech citizens.

The Czech Republic was the focus of the interest of actors with links to Russian and Chinese state structures in cyberspace as well. Czech institutions and citizens were targets of several cyberespionage campaigns with the most serious one being the compromising of the unclassified network of the Ministry of Foreign Affair.

In 2018, the BIS did not identify serious hostile activities of intelligence services of other states, with the exception of the activities of Iranian intelligence services that are described below.

Russian Intelligence Services

In 2018, members and cooperators of all Russian intelligence services (the SVR external civilian intelligence service, the GRU external military intelligence service and the FSB internal security and intelligence service) were present in the Czech Republic and conducted intelligence activity here. The oversized personnel numbers of the Russian diplomatic mission in the Czech Republic remain a long-term security problem and increase the threat for Czech citizens of being faced with contact with a foreign intelligence service.

Russia's intelligence capacity in the Czech Republic was partially weakened by the Czech reaction to the nerve agent Novichok attack in Salisbury, Great Britain. Such a substance was used to poison Sergei Skripal and his daughter in Great Britain in March 2018. After Great Britain had announced details of the attack, Russia tried to create the international impression that the toxic substance used came from other countries, primarily from the Czech Republic. According to the findings of the BIS, no entity in the Czech Republic developed, manufactured or stored the nerve agent used in Great Britain. With respect to the fact that in the past individuals, who participated in the attack, had stayed in the Czech Republic and in connection with the British request for a collective allied course of action, the BIS prepared relevant source information that was then used in the process leading to the expulsion of three Russian undeclared intelligence officers.

In accordance with the hybrid strategy, with which Russia tries to influence the decision-making of foreign-political representatives, Russian intelligence officers strived to establish links and to cultivate an influence basis close to politicians, who can affect the development in Russia's areas of interest.

The Russian diplomatic mission and the residency of one Russian intelligence service remained interested in the Russian compatriot community. By collection information and building influence networks, Russian state structures tried to primarily marginalize anti-Kremlin compatriot entities and to increase the influence of those compatriot entities that sympathize with the current Russian political representation.

In 2018, the Czech Republic remained one of the stages for subversive activities directed by Russian state structures against Ukraine's political sovereignty and territorial integrity. These activities showed signs of active measures. Russia's practice has been for many years the effort to covertly create and fuel in target countries social tensions related to substitute topics, which however in the end affect the whole balance of power. The use of this practice intensified in connection with the geopolitical development framed by the 2014 annexation of Crimea. The significant increase in public attention directed at this practice was then reflected in the discussion on Russia's so-called hybrid approach to warfare, or more specifically foreign policy.

In cooperation with a partner organization, the BIS also acquired information on the activities of the Russian FSB intelligence service that was building an ICT infrastructure covertly in the Czech Republic. This infrastructure was a part of a larger system usable to cover FSB cyber and information operations of local and global scope. In cooperation with the Police of the Czech Republic the network was destroyed and FSB was thus prevented from its activities against Czech Republic and allies´ interests.

Chinese Intelligence Services

Both the intensity and scale of Chinese intelligence activities grew and they posed a threat to the interests and security of the Czech Republic in 2018. All of the most important Chinese intelligence services were active in the Czech Republic – the external military service (MID), the International Department of Central Committee of the Communist Party of China (CPC/ID), the Ministry of State Security (MSS) and the Ministry of Public Security (MPS). Chinese career diplomats continued to resort to the use of pressure to advance China's interests.

In the context of Chinese activities aimed at the Czech academia, security bodies and state administration, the BIS identified a growing number of Chinese invitations addressed to Czech citizens for trainings, seminars and excursions. China offers to cover all expenses for the invited individuals (transport, accommodation, food allowance, registration fees) and even to give Czech guests spending money. Such journeys ensure a whole range of benefits for China – the country thus establishes a contact network of individuals, who will regard it with favor, or more specifically feel that they "owe China something" and will be willing to be forthcoming towards China. From an intelligence point of view, the most risky aspect is the physical presence of the guest in China. Chinese intelligence services usually use the stay of persons of interest in China or in a third country (so usually not in the individual's country of origin) to approach them for cooperation.

In order to approach potential Czech sources or cooperators (academic workers, students, civil servants and other individuals with access to sensitive information), Chinese intelligence services use in the Czech Republic among other things the LinkedIn network as well.

A significant element of China's intelligence activities in the Czech Republic was the continuing efforts to disrupt Czech-Taiwanese political and economic relations. In 2018, Chinese representatives

put maximum effort into acquiring information on the cooperation in order to react quickly with the aim to weaken Czech contacts with Taiwan.

Russian and Chinese Cyberespionage Activities

The Compromising of the Ministry of Foreign Affairs Network

In 2018, an inquiry was carried out into the vast compromising of the unclassified network of the Ministry of Foreign Affairs. Based on the intelligence obtained it is highly likely that it was a Russian cyberespionage campaign. The vector of this espionage attack was a Czech representative office abroad that had been compromised at the end of 2017 already.

In the primary attack phase, perpetrators compromised several end computers of the unclassified network of the representative office. Further inquiries uncovered attackers' attempts to use the privilege escalation and lateral movement technique. Perpetrators also tried to secure a permanent covert access to the attacked system.

The BIS also acquired information on another, unrelated incident – on a compromising of selected computer stations of the unclassified network of the Ministry of Foreign Affairs by several types of malware. Based on various indicators, it was strongly probable to connect them to activities of a Chinese cyberespionage group. Traces of carefully hidden activities could be traced several years back and in that time, attackers managed to exfiltrate many documents on topics that correspond to the interests of the cyberespionage actors in question.

Because of its purview, the Ministry of Foreign Affairs constantly faces more or less sophisticated cyberattacks conducted not only by state actors. It is therefore necessary to improve processes and communication security further and to ensure such technical measures that will enable an effective reaction to attacks.

Attacks of the APT28/Sofacy Cyberespionage Campaign against Members of the Czech Armed Forces

In 2018, the BIS informed its entitled addressees about cases of the compromising of private e-mail accounts belonging to members of the Czech Armed Forces and about the fact that these e-mail accounts were most likely compromised by the Russian APT28/Sofacy cyberespionage campaign. Even though the attackers did not acquire any information classified under Act No. 412/2005 Coll., on the Protection of Classified Information, they gained access to personal and sensitive data (place of residence, invoices, vacation destinations and dates, family background, many contact details, etc.). In the future, they can misuse this information through social engineering for further attacks, not only against members of the Czech Armed Forces.

When looking into the activities of the APT28/Sofacy cyberespionage campaign in the Czech Republic, the BIS also uncovered a case of a compromised e-mail account belonging to a member of the Czech Armed Forces. The account was being searched automatically via its IMAP or POP3 protocol link to another e-mail address controlled by the attackers. This method of linking e-mail accounts is very effective. In many Czech e-mail services, the victim cannot detect it because providers do not allow their clients to check, from which IP addresses their account is being accessed.

Aside from the cases of the compromising of personal accounts of Czech Armed Forces members, the BIS also worked on several other similar cases of e-mail accounts suspected of being compromised by the Russian APT28/Sofacy cyberespionage campaign in 2018.

2.2 Protection of the Constitutionality and of the Democratic Foundations

Activities of the spectrum of pro-Russian activists, who were involved in spreading disinformation, posed the gravest threat to the constitutionality of the Czech Republic in 2018. The term "pro-Russian activists" is not meant to include all individuals with pro-Russian attitudes, but primarily people, who through their activities wittingly or unwittingly directly assist a foreign power.

The BIS continued to monitor the activities of paramilitary and militia groups that by their mere existence cast doubt on the state monopoly on the use of force in its own territory. Militias stagnated in 2018, which had to do with social development (primarily with fears of the arrival of a larger number of migrants to the Czech Republic not being realized) and with the internal state of individual groups. Primarily groups that operate on local level proved to be truly functional, but only in certain regions of the Czech Republic. These groups attracted fewer radicals firmly anchored in a specific ideology and proved more attractive to people, who viewed combat training and their activities in militia groups as a hobby. The activities of paramilitary and militia groups thus did not pose a real direct threat to the democratic foundations and security of the Czech Republic.

Last year also confirmed that traditional right-wing or left-wing extremist groups do not pose a security threat now either. The right-wing extremist scene has been in crisis for several years now and we do not expect a significant change in the coming years. The popularity and support of politically active right-wing extremists was minimal. Membership of left-wing anti-authoritarian platforms has been small in numbers for a long time and it has stagnated as well. Militant anarchists were not active in the Czech Republic. The current state of both scenes is also illustrated by the fact that violent clashes between left-wing and right-wing extremists have practically disappeared.

Pro-Russian Activists

In recent years, pro-Russian activists opposed the political order of the Czech Republic and its membership in the EU and NATO more intensively, more conceptually and more systematically. In their activities, they participate in promoting topics that are manufactured or supported by a foreign power. The significance of existing threats is often inflated and imaginary problems created. Incentives to conduct actions against allied interests are frequent as well. By using misleading, manipulative or false statements, pro-Russian activists influence public opinion and create and maintain fear and tension in the society. That contributes to society's polarization and radicalization and it undermines public trust in the principles of free democratic state. Topics that serve the interests of a foreign power can put pressure on political representatives and decision-making systems or processes.

Pro-Russian activists (whether wittingly or unwittingly) thus supported Russia's influence operations and advocated Russian interests to the detriment of Czech interests. Large numbers of pro-Russian activists are motivated by ideological affinity, admiration of the President Putin's regime or general adoration of Russia. There are, however, indications concerning certain individuals of their direct links to Russian state structures or of them being directed by Russian intelligence services.

The spectrum of pro-Russian activists consists of a wide range of entities with no regard to the right-left division and formal position. The spectrum encompasses members of various nationalist and populist movements, some political parties, registered associations, informal initiatives, groups and unorganized individuals, including groups and people that came from past anti-immigration movements. The spectrum also consists of media presenting themselves as independent or alternative, individuals, who strive for Ukraine's territorial disintegration, and Cossack groups. All these groups were linked to one another. Thanks to their common fondness towards Russia, their representatives were able to cooperate regardless of their different ideological beliefs.

Pro-Russian activists influenced public opinion e.g. by spreading various conspiracy theories and pro-Russian propaganda. To achieve that, they used primarily the internet, social networks, their own internet video channels or the so-called independent/alternative media that are now the main producers of disinformation benefitting Russia.

Some pro-Russian activists focused on public rallies, debates and petitions aimed against the EU, NATO and against the decisions of these international structures related to immigration to Europe.

Paramilitary and Militia Groups

Even though the BIS assesses the general threat stemming from militia activities as not overly significant, certain aspects of the activities of these groups and their members carried potential risk. Among members of these groups were individuals inclined to support conspiracy theories or to have radical tendencies. In connection with their positive relationship and attitudes to weapons, these individuals posed a potential risk and their behavior was unpredictable.

Because of their significant anti-Western orientation, members of paramilitary groups also contributed to the spread of pro-Russian propaganda and related conspiracy narratives. After the topic of migration and the related danger posed by refugees had grown gradually quiet in the society, many members of paramilitary groups focused on creating the impression of a threat of an armed conflict between the West and Russia (even though they still often used the migration topic as well).

In order to gain legitimacy, paramilitary groups still tried to organize various public awareness events and establish contacts and cooperation with representatives of municipalities and security forces on regional level in the area of maintaining security in the streets. A significant goal of militia representatives in 2018 still was to legalize them by incorporating them into the legal order of the Czech Republic.

Traditional Political Extremism

Similar to previous years, criticism of the migration policy, strong anti-EU attitudes, critical statements against Muslims and distancing themselves from human-rights activists or NGOs, were among dominant topics of right-wing extremists. Anti-Roma language, which had been on the edge of their interest for several years, was also reactivated.

The year 2018 showed more than ever that a growing spectrum of entities uses language and topics previously reserved for "orthodox" right-wing extremists. Public tolerance towards this language grew considerably and there was a significant shift in the threshold, of what xenophobic or

racist language can be a part of the political mainstream. This shift is one of the reasons for the decline of traditional extremist groups that are losing space, in which they could present themselves as unique bearers of radical ideas.

Public activities of anarchist-autonomous collectives stagnated and organized primarily smaller events aimed at the movement itself, such as lectures, activist meetings, solidarity and commemorative events, concerts or happenings. The majority of the anarchist-autonomous scene rejected violence and the so-called insurrectionary anarchism.

Militant anarchists were practically inactive and they did not claim any direct operations. Their minimal activity was also apparent on the internet, where they only expressed support to anarchists detained abroad. One exception was the publishing of instructions on how to anonymize one's internet activity.

The radical communist part of the left-wing extremist scene is fragmented, its ideas are disparate and it faces long-term stagnation. Its representatives were aware of that and there were several (in the end unsuccessful) attempts to reverse this state and mobilize the scene in 2018. Some radical communists saw a closer cooperation across the "progressive" left-wing scene as a solution and considered the creation of a wider left-wing front. Individual entities did not hold larger events, but often cooperated on the organization of smaller events.

2.3 Terrorism and Organized Crime

Terrorism

The situation pertaining to terrorism and Islamist radicalization was calm in the Czech Republic in 2018. The BIS monitored situation development in the Muslim population and looked into signals about the potential presence of Islamist radicals in the Czech Republic in 2018. Specific direct risks in relation to the Czech Republic have not been confirmed in any of the cases. The BIS also looked into several further suspicious cases related to the fight against terrorism financing. Intelligence suggesting that the Czech Republic might serve as a logistical or other base for international terrorism was not acquired in this area either.

The BIS focused on radical Muslims, who had left the Czech Republic in past years in order to join terrorist organizations in Syria and Iraq. We were able to confirm the death of one of these foreign fighters. The BIS also secured and passed to the entitled addressees intelligence on the radical imam Samer Shehadeh, who was extradited to the Czech Republic based on an international arrest warrant for the charges of supporting terrorism. With his radical beliefs, Shehadeh influenced his brother and his Muslim wife (both are Czech citizens) and subsequently helped them with the organization of their journey and joining of al-Qaeda's Syrian branch.

The BIS also continued to acquire information on risk Maghrebans, manifestations of Islamist radicalization in a part of the Kazakh community, Libyan patients with links to Islamist networks and on radicalization potential of a part of the Muslim community in Prague.

The Maghrebi community in decentralized and lacks authorities that would prevent radicalization manifestations. We perceive the following risk indicators among Maghrebans: their disinterest in integration into society, criminal activity, efforts to legalize their stay in the Czech

Republic through marriage (or relationship) of convenience and financial problems. We came across several individuals with manifestations of radicalization among people showing these signs and we conducted appropriate intelligence work on them.

A part of the Kazakh community continued to pose a security risk. Its members still refuse to integrate into the Czech society and adhere to a specific form of Islamism. The potential to spread Islamist radicalization of these Muslims in the Czech Republic was limited.

So-called Libyan patients come to the Czech Republic for treatment within a program for injured veterans paid by Libya. In cooperation with other security forces of the Czech Republic, the BIS helped to identify several individuals with links to Islamist structures in Libya. Measures to prevent their further entry into the Czech Republic were imposed on these Libyan patients, people accompanying them and treatment facilitators.

The affairs of individual organizations that bring together Muslims in the Czech Republic were influenced by their dynamic internal development. The Muslim community in Prague went through the most significant transformation. Muslim organizations continued to face personnel and financial problems. Despite efforts of various groups to gain influence over these organizations, the long-term moderate character of the Muslim community was maintained.

Because of the past findings on Iran's state support of terrorism, the BIS continued to focus on the activities of Iranian intelligence services in the Czech Republic. They operated in our country in 2018 as well. Cooperation on various business projects continued within the development of Czech-Iranian relations. However, such cooperation also has to do with security because there might be individuals, who are linked to Iran's security forces to a varying extent, among regular Iranian businessmen.

At the beginning of 2018, the BIS successfully brought to the end an operation monitoring the infrastructure of Hezbollah's cyberespionage campaign located in the Czech Republic. This cyberespionage campaign was not aimed at Czech citizens, but primarily on victims from the Middle East.

The attackers operated from Lebanon and they were using several servers in the Czech Republic in 2017 and 2018. The primary function of these servers was to distribute an espionage application for the mobile Android operation system. They used social engineering and tried to persuade their targets to install the modified application posing as a legitimate communication program using fake profiles of attractive women on social networks. After installation, the application started to send sensitive data from the phone to attackers' servers.

Based on acquired intelligence, the attack infrastructure used to spread the malicious code was eliminated at the beginning of 2018.

The BIS also worked on the impact of tensions in the Middle East on the security situation in the Czech Republic. We did not acquire intelligence suggesting the transfer of these tensions to the Czech Republic or intelligence suggesting the threat of a terrorist attack being committed in the Czech Republic as a result of these tensions.

Organized Crime

Similar to previous years, the BIS continued to monitor the situation of the Visapoint information system run by the Ministry of Foreign Affairs. The system was meant to ease for visa applicants the registration to free personal appointments at Czech embassies and to eliminate scheming with places in lines. The system was launched in 2009, but it did not meet the expectations because the problem with scheming only moved from the physical world to the cyber world.

Intermediaries, who registered appointments in Visapoint in exchange for payment, tried by certain visa types to fill all free dates with fictional individuals, thus preventing real applicants, who were not within their reach, to register. The intermediaries then demanded up to several thousand euros per person for a place in the electronic line. The dominant intermediary eventually managed to control practically fully the access to visa appointments at several Czech embassies using automated tools. By this conduct, this intermediary prevented legitimate interested persons from lodging their visa applications and these individuals were subsequently forced to buy free appointment dates for hundreds or thousands of euros per person. By using his IT knowledge, this intermediary had been influencing the Czech visa system for a long time and systematically with the aim to enrich himself. The intermediary gained millions of Czech crowns a year.

The termination of Visapoint's operation and the change in the way free appointment dates are registered complicated for this intermediary the way to his enrichment. However, the intermediary still tried to find a way to block appointment dates at Czech embassies.

In September 2018, detectives from the organized crime section of the National Centre against Organized Crime (in Czech: *Národní centrála proti organizovanému zločinu*, NCOZ) arrested eight foreigners from the Russian Federation and the Socialist Republic of Vietnam. They are suspected of organizing criminal activity related to lodging applications for residence permits in the Czech Republic by citizens of the Socialist Republic of Vietnam. The BIS closely cooperated with the Police of the Czech Republic on this case.

2.4 Activities that Jeopardize the Security and Major Economic Interests

Proliferation of Weapons of Mass Destruction and Trade in Military Material

The Czech Republic has made an international commitment not to participate in proliferation of weapons of mass destruction (WMD) and their carriers and to minimize risks related to international trade in conventional weapons, military material, explosives and dual-use goods. The Czech Republic is a member of all the International Control Regimes (ICRs)[1] that deal with nuclear, chemical and biological (bacteriological and toxin) WMDs and their carriers and other internationally controlled items.

[1] 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 the United Nations Security Council Resolution No. 1540 (2004).

The task of the BIS in this area is to acquire and analyse information and inform in a timely manner about specific incidents, phenomena and trends connected to foreign trade in controlled items and to circumventing or violating other obligations of the Czech Republic arising from international sanctions imposed on respective countries or entities[2].

In the Czech Republic, WMDs are completely excluded from trade and other controlled items are subject to legal regulations[3]. The Czech Republic is nevertheless seen among the countries that pose the gravest proliferation threat as a traditionally engineering country with quality products, materials and technologies for affordable prices. In 2018, the BIS therefore also identified many cases of such countries trying to buy in the Czech Republic engineering devices, special materials, technologies and know-how that might be of use in research and development of their own WMDs. North Korea, Syria, Iran and Pakistan pose the gravest proliferation threat.

International sanctions are an effective measure against trade in WMDs and controlled items. Sanctions are still imposed on North Korea and Syria. Despite sanctions being softened on Iran in the area of nuclear technologies, the ban on supplies of conventional weapons and goods for the Iranian nuclear program remains in place. International weapons sanctions also pertained to several countries in the Middle East, Southeast Asia and Caucasus or African countries. Since August 2014, EU sanctions have been imposed on supplies to Russian arms factories and weapons-programs entities as well.

Entities from Russia, China and other countries with unstable and repressive regimes and from countries, where armed conflicts are taking place, expressed interest in military material, weapons and explosives or in special components that can be used in the development and manufacture of e.g. UAVs (drones) for military purposes. Trade in UAV components carries the risk of their re-export to other countries that pose a proliferation threat.

When procuring goods with necessary technical parameters, companies from states that pose a proliferation threat are able to prepare complicated trade routes via third countries and to adapt payments to the re-export of goods with the aim to prevent identification of such trade routes and of all companies involved. Breaking or circumventing international commitments would damage security, economic interests and the good reputation of the Czech Republic and weaken its international position.

Protection of Major Economic Interests

In 2018, the BIS focused increasingly on negative phenomena directed against independent and proper performance of the regulatory and oversight role of central state authorities. Another important topic were risks associated with economic activities of entities linked to foreign powers that used these activities to advocate their foreign-political and strategic goals.

---

[2] Section 5, Paragraph 4 of Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended.

[3] 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.

In remaining areas, the structure of monitored phenomena that jeopardize major economic interests of the Czech Republic was similar to previous years. The BIS described a whole range of cases of clientelism, illegitimate lobbing or efforts to circumvent the law that were of similar nature to cases identified in the past. The BIS also focused on consequences of such activities and the capabilities of the state or state-controlled companies to deal with these consequences.

The BIS identified several serious cases of interference in the operation of regulatory and oversight authorities. Certain entities were partially successful in their efforts to influence key decisions of authorities to the benefit of their specific interests. In order to achieve that, they used a wide spectrum of methods ranging from legal lobbing, covert influencing of the media landscape to efforts to control directly the decision-making of authorities through insiders on high positions in their structures. A common part of the strategy of these entities was the effort to use various ways to get access to key inside information from the authorities, such as upcoming decisions or planned analyses used by the authorities to determine further steps.

The BIS considers this interference to be a grave danger to major economic interests of the Czech Republic. Regulatory and oversight authorities have a significant influence on conditions in whole sectors and the manipulation with their decision-making has a significant negative impact on the trust of disadvantaged entities (both business entities and wide groups of consumers as well) in the capability of the state to ensure a fair economic environment. Such a state might have a negative effect on the investment climate and lower the attractiveness of the Czech Republic to renowned foreign investors.

The ability of some of these authorities to perform their duties was also impaired due to personnel instability and disputes among individual representatives. In several cases, these disputes led to questions about the legitimacy of the decision-making of the whole authority. Mutual animosity and resulting efforts to harm one's opponents paved the way for illegitimate lobbying activities. Efforts to gain powerful backing were also part of these disputes. That was connected to the risk that an expression of support will be or has been exchanged already for advantages in the authority's decision-making.

The BIS also identified efforts of entities that are subject to regulation and oversight to circumvent legal regulations. In one sector that is subject to regulation, deals were made pertaining to pricing and access to contracts. In another strategic sector, important standards were circumvented in such a way that would allow participating entities to use the cover of legal economic activity in order to misuse their presence on the Czech market to achieve goals that are undesirable to the Czech Republic. In this respect, the risk was posed primarily by entities financed with capital from countries, in which the state administration advances its interests abroad through a strong influence on the decision-making in companies.

The identification and assessment of risks that might arise from links of economic entities active in the Czech Republic to foreign powers therefore became an important topic. It was confirmed that the less democratic system there is in the country, from which the capital originates, the higher the risk of misuse of resources for foreign-political goals. Authoritarian countries are by their nature more successful in advocating their influence in private companies more effectively. By using a range of formal and informal measures, they are able to force these companies to suppress their own economic interests and give priority to state political, military or intelligence goals when needed. These goals can

be in conflict with the interests of the Czech Republic e.g. in the area of the protection of key technologies or the information and energy security.

The misuse of economic activity of a foreign company in the Czech Republic can pertain to any economic relationship. Risks can be linked to supplies of sensitive goods or services, investments into assets related to security and to buying into strategic companies. In some of these cases, the Czech Republic had insufficient instruments to face these threats, or it used available tools only to a limited extent. However, when applying any regulations, it is necessary to take into account that the Czech Republic has a very open economy, in which the activities of foreign companies and the presence of foreign capital constitute an important development factor. When assessing risks, it is therefore necessary to analyze not only the will and ability of a foreign entity to conduct activities against the interests of the Czech Republic, but also whether the specific activity can really enable the misuse of these abilities against the interests of the Czech Republic.

The state also faced enduring problems with the administration and construction of ICT systems. Risks arose primarily from the dependence of many state contracting authorities on long-term technology suppliers, which significantly limited negotiating options related to better terms or the replacement of current systems with different ones.

The BIS also identified risks that could have jeopardized cyber security in an institution that operates several information systems, which are part of the critical information infrastructure. These security deficiencies were not dealt with over a long period in a systematic way and some of them persisted for a long time, while other new problems manifested. Experienced employees, who had knowledge and skills needed for administration of that authority's systems, gradually left the department responsible for information technologies in that institution and appropriate replacement could not be found. Furthermore, officials from key departments did not possess necessary knowledge and largely ignored the issue of cyber security.

In several cases, long-standing problems caused by low quality business relationships, which interfered with the operation of a state authority or certain state-controlled companies, still were not resolved in 2018. Legal, technological or foreign-political intricacy of circumstances was a typical obstacle in the effort to find an acceptable solution. However, passivity, imperfect cooperation or rivalry between individual responsible state actors also contributed to delays in some cases.

The BIS also identified several cases of clientelism or serious conflict of interests. They were often activities that had traits of a criminal offence according to many characteristics. In certain identified cases, they were accompanied by the main actors' belief that they were untouchable due to their contacts with lobbyists and various advisors, who sold them their often intentionally overrated influence on state institutions. The BIS gave criminally relevant intelligence to law-enforcement authorities.

3 Protection of Classified Information

3.1 Administrative Security

The year 2018 brought no significant changes in the area of protection of classified information. Similar to 2017, the BIS drew up expert opinions, assessed documents in relation to classification in accordance with Act No. 412/2005 Coll., interpreted items listed as classified in the BIS sphere of powers and relevant internal regulations and provided methodical help to organizational units.

3.2 Security of Information and Communication Systems

When managing the security of information systems in the BIS, continuous improvement of ICT system security and service provision, both in systems for processing classified and unclassified information, are emphasized. 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.

In 2018, security documentation was updated and the information system for processing information classified as Secret was successfully re-certified. Technologies for tracking user access to data are still being perfected in the information system.

All users of certified information systems are trained in accordance with Act No. 412/2005 Coll. before their first access to the system and then undergo annual trainings.

In 2018, the BIS detected no serious incidents or a case of compromising in the operation of information and communication systems or cryptographic devices. Regular checks of cryptographic material did not find any deficiencies in the management and manipulation with this material.

3.3 Physical Security

In the area of physical security, the BIS continued to improve 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. 528/2005 Coll., as amended.

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 of classified information in emergencies, Plans for Building and Area Security, which are part of Security Projects, were 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 service activities as well.

Close cooperation with the Office for Foreign Relations and Information and with the Military Intelligence focused on counterespionage, cyber security, 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 based on requests of the Police, or of the relevant public prosecutor's office, pertaining to specific criminal proceedings.

One of the forms 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 a credibility assessment of natural persons conducted by the Police of the Czech Republic. Based on Police requests for cooperation in assessing credibility of natural persons, the BIS issued opinions on individual applicants for the ÚCL certificate.

The cooperation with the National Centre against Organized Crime in 2018 had the form of intelligence exchange pertaining to the screening of entities of interest. Findings in the area of economic crime and cyber security were provided as well.

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 cooperates 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 (in Czech: *Národní bezpečnostní úřad – NBÚ*) 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.

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

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 passes information in reaction to numerous and repeated NBÚ requests on 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.).

In the fight against terrorism, the BIS played an active role in regular meetings of the working platform meant to collect, process and share information on risk individuals suspected of activities related to terrorism in 2018. The platform is called the National Contact Point for Terrorism (in Czech: *Národní kontaktní bod pro terorismus*) and it falls under the remit of the National Centre against Organized Crime. The National Centre against Organized Crime, the BIS, the Office for Foreign Relations and Information and the Military Intelligence are partners within the National Contact Point for Terrorism. The BIS also played an active role in the Joint Intelligence Group (in Czech: *Společná zpravodajská skupina*), the permanent working body of the Committee for Intelligence Activity (in Czech: *Výbor pro zpravodajskou činnost*), the aim 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 nearly 140 000 natural and more than 800 legal persons in total.

In 2015, an 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, came into force. These screenings include a credibility assessment of the natural persons. The BIS processed requests pertaining to more than 7 000 individuals within this agenda.

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 2018, the BIS screened more than 1 800 000 applications.

BIS representatives took part in meetings of National Security Council (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 Defense Planning and Committee for Civil Emergency Planning. Expert departments of the BIS drew up opinions and comments on materials of all Committees and the National Security Council.

Active cooperation was also conducted within the Interagency Body for the Fight against Illegal Employing 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 2018, the BIS also cooperated intensively with the National Cyber and Information Security Agency, the General Inspection of Security Forces (in Czech: *Generální inspekce bezpečnostních sborů*), the Financial Analytical Office (in Czech: *Finanční analytický úřad*), the Customs Administration of the Czech Republic (in Czech: *Celní správa ČR*), the General Directorate of Customs (in Czech: *Generální ředitelství cel*), the Prison Service of the Czech Republic (in Czech: *Vězeňská služba ČR*), the General Financial Directorate (in Czech: *Generální finanční ředitelství*) and courts and public prosecutors.

Cooperation with other state 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 directorates of customs. The cooperation continued with customs administration bodies on risks of potential transport of controlled items, primarily military material and dual-use items, to sanctioned countries. In specific cases, cooperation was conducted with the Ministry of the Interior, Ministry of Industry and Trade Licensing Administration and with the State Office for Nuclear Safety (in Czech: *Státní úřad pro jadernou bezpečnost*) and their subordinate organizations, also in ongoing authorization and licensing proceedings and in providing information on the compliance with license conditions and international control regimes. The BIS also worked on exports of goods that have characteristics of items under international control regimes from the Czech Republic to risk countries.

In addition to providing and exchanging information, the BIS gives to other state authorities generalized findings and recommendations when commenting on various legislative and non-legislative documents. Furthermore, the BIS organizes various training courses, holds consultations, 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. 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 700 international strategic and expert meetings.

The level of international information exchange was similar to 2017. 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 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. 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. This shows that 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. 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 the special oversight body established in accordance with Act No. 154/1994 Coll., on the Security Information Service, as amended (please see below).

The separate 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 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.

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 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, 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 60 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 reserve special conditions related to their manner.

BIS operation is also subject to judicial oversight in cases of the use of intelligence technology in accordance with Act No. 154/1994 Coll. Its Section 9 and subsequent paragraphs 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 BIS requests for reports from banks, including foreign banks, and savings and credit cooperatives on matters related to their clients 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 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 BIS. In 2018, two external audits were conducted – an audit by the Supreme Audit Office (in Czech: *Nejvyšší kontrolní úřad - NKÚ*) focused on the assets and funds allocated for the operation of the BIS. The second case was an audit of the compliance with requirements and measures stipulated in Act No. 258/2000 Coll., on Protection of Public Health, in Government Regulation No. 361/2007 Coll., on the Conditions for Occupational Health Protection, and in related legal regulations.

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 BIS Director. In 2018, the internal audit service completed three audits focused on commissioning public tenders, management of assets allocated to the BIS, and on monitoring the compliance with measures that arose from internal audit recommendations and were approved by the BIS Director.

Other BIS expert units conducted 45 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 12 inspections of persons (officially on a contract of service) temporarily unable to work.

Employees of the archive and of the control group carried out 45 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.

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.

In the area of Investigation of Conduct Suspected of Having the Traits of a Misdemeanor and of a Disciplinary Infraction, the BIS Inspection Department focuses primarily on traffic offences on public roads. 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 of having traits of a misdemeanor.

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

Complaints, notifications and suggestions that the BIS Inspection Department investigated in 2018 were submitted mostly by external entities. Compared to 2017, the number of investigated notifications and suggestions increased substantially by 89.7%. 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 misdemeanor proceedings. The number of processed requests corresponds to the long-term situation.

8 Budget

The budget of the BIS was stipulated by Act No. 474/2017 Coll., on the State Budget of the Czech Republic for 2018.

Salaries and equipment payments traditionally accounted for the majority of total expenditures. Their increase was affected by the adjustment of basic wage rates in November 2017 and the changes in overtime payments since 2018. Personnel expenditures also include severance benefits, i.e. mandatory payments for Service members whose service has ended. Starting in 2018, new members receive recruitment subsidies.

Further regular expenditures included mainly standard expenditures for services, standard material, fuels and electrical power expenses ensuring the normal functioning of the BIS. 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 information and communication technologies. Their aim was to ensure the necessary performance of server and communication technologies, disk capacities and the development of software solutions for the support of intelligence processing. A significant part of capital investment expenditures was allocated to construction. The rest of capital investment expenditures was invested in intelligence technology. Further expenditures were allocated to necessary replacement of means of transport.

The budget 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 areas of physical, administrative and personnel security, and in the area of security of information and communication systems. The need to consider these facts in the whole spectrum of BIS activities leads to much expenditures, which are absent or very limited in other organizational units of the state.

Basic operational and development needs of the BIS were fully covered with regard to available capacity potential. In terms of personnel, the budget improved and allowed a 4.8% increase in the number of occupied service posts in 2018 compared to the previous year. The budget also financed development activities in the area of intelligence technology and information and communication technologies.

A detailed report on BIS economic management structure in 2018 in accordance with the relevant regulation 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 2018 (CZK thousands)

	Approved budget	Amended budget	Real data
Total revenues	150 000	150 000	202 265
Total expenditures	2 007 592	2 005 415	1 649 973