

# Annual Report of the Security Information Service for 2015

## Table of Contents

<b>1. The Nature and Scope of Intelligence Activities .....</b>	<b>2</b>
<b>2. Intelligence Activities and Findings .....</b>	<b>3</b>
2.1. Protection of Major Economic Interests.....	4
2.2. Organized Crime .....	5
2.3. Counterintelligence Activities .....	8
2.4. Protection of the Constitutionality and the of the Democratic Foundations of the Czech Republic.....	10
2.5. Terrorism.....	13
2.6. Proliferation of Weapons of Mass Destruction .....	14
2.7. Cybersecurity .....	15
<b>3. Protection of Classified Information .....</b>	<b>18</b>
3.1. Administrative Security.....	18
3.2. Security of Information and Communication Systems .....	18
3.3. Physical Security.....	18
3.4. Crisis Management .....	18
<b>4. Cooperation with Intelligence Services of the Czech Republic and with other State Authorities</b>	<b>19</b>
4.1. Cooperation with Intelligence Services of the Czech Republic.....	19
4.2. Cooperation with the Police of the Czech Republic.....	19
4.3. Cooperation with other State Authorities and Institutions.....	20
<b>5. Cooperation with Intelligence Services of Foreign Powers .....</b>	<b>22</b>
<b>6. Oversight .....</b>	<b>23</b>
6.1. External Oversight.....	24
6.2. Internal Audit .....	24
<b>7. Maintenance of Discipline; Handling Requests and Complaints.....</b>	<b>25</b>
7.1. Investigation of Conduct Suspected of Having the Traits of a Misdemeanor, of a Disciplinary Infraction, and of other Infractions.....	25
7.2. Investigations of Complaints and Notifications .....	25
<b>8. Budget</b>	<b>26</b>

## 1. The Nature and Scope of Intelligence Activities

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

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

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

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

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

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

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

## 2. Intelligence Activities and Findings

A summary of all the intelligence activities, in which the BIS engaged in 2015, is part of the classified *Report on the Activities of the Security Information Service for 2015* – a report the BIS submits to the President of the Czech Republic and to the Government in accordance with Section 8, Paragraph 1 of Act No. 153/1994.

During the course of the year, again in accordance with Section 8, Paragraph 1 of Act No. 153/1994, the BIS informed entitled addressees about individual intelligence findings and the results of analyses, on which the overview of its activities in this public annual report is based. In 2015, the BIS submitted more than 600 documents to the President and Cabinet members. More than 300 documents were sent to relevant state authorities, the Police of the Czech Republic, the Office for Foreign Relations and Information (in Czech: *Úřad pro zahraniční styky a informace – ÚZSI*), and to Military Intelligence (in Czech: *Vojenské zpravodajství – VZ*).

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

The BIS cooperates also with other state bodies (e.g. the Department for Asylum and Migration at the Ministry of the Interior, the Ministry of Foreign Affairs, the Ministry of Industry and Trade Licensing Administration) in areas falling under the remit of these authorities, e.g. residence permits in the Czech Republic, the MEDEVAC project, the arrangement of employment, international protection stipulated by the Asylum Act, or foreign trade in military equipment. In 2015, the BIS processed requests for information concerning almost 100 000 natural and more than 1 200 legal persons.

Government resolution 18 of 14 January 2015 provided for the resettlement of 15 Syrian families from Jordan and government resolution 1052 of 14 December 2015 provided for the resettlement of Christian refugees from Iraq and Lebanon chosen by the Generation 21 Foundation. In relation to these projects, the BIS screened almost 200 individuals.

Government resolution 325 of 6 May 2015 introduced the project “New Elites for Syria - a scholarship program provided by the Government of the Czech Republic to Syrian refugees” aimed at providing university education to individuals, who will contribute to the restoration of the Syrian state after the conflict ends. In relation to this project, the BIS screened almost 30 individuals.

In 2015, an amendment of Act 49/1997, on Civil Aviation, came into force, which stipulates provisions regarding reliability certificates issued to legal persons by the Civil Aviation Authority (in Czech: *Úřad pro civilní letectví - UCL*). These screenings include a credibility assessment of the legal persons conducted by the Czech Police. In relation to this matter, the BIS processed requests concerning almost 16 000 individuals.

In compliance with Article 9 of the Convention, implementing the Schengen Agreement the BIS, as the responsible Czech intelligence service, submits opinions on Schengen visa applications. In 2015, the BIS screened more than 1 000 000 applications.

## 2.1. Protection of Major Economic Interests

Threats posed to major economic interests in 2015 were similar to those in previous years and were characterized by negative consequences of errors made in the past. Poorly set contract conditions accepted by some state entities in various sectors (energy industry, banking, road transport, ICT) are a major issue. Some of these contracts were signed more than 10 years ago.

The dilatoriness of responsible individuals after the contracts were signed contributes to the gravity of the problem. In a number of cases, these individuals lacked the initiative to supervise and assess the concluded contracts and possibly change their conditions. Therefore, the situation often became critical and it became exceedingly difficult or completely impossible for state representatives to achieve a satisfactory solution to the problem. An example of such a problem is the company commissioned with the administration and protection of a part of Czech strategic oil reserves.

A number of problems also accompanied the provision of ICT services. Some state entities became greatly dependent on their suppliers. In one case, services provided to a key regulatory authority, which are crucial for the operation of the sector in question, were suspended. Even though the management of the regulatory authority was aware of the problem, the matter was not addressed in time.

The BIS focused on describing the relations and intentions of individuals, who contributed to a problematic situation and had significant influence. Some individuals, who left civil service (e.g. were made redundant), attempted to renew their influence on state entities. In some cases, they succeeded by making use of previous contacts and exploiting the loyalty of current civil servants. This affects the state's ability to solve existing problems. The BIS has been informing entitled addressees about these problems and about further derogatory developments; however, it cannot directly influence the solution to the problems. The BIS collects, evaluates and hands over information that can be used for at least a partial elimination of consequences.

Sensitive information leaks used to obtain benefits for the counterparty also often significantly damaged state interests. Leaks were caused not only by individuals seeking to secure private gain, but also by an insufficient awareness about the need to protect sensitive information not considered classified by special legislation.

Major economic interests are of interest also to foreign intelligence services, which aim to gradually win the loyalty of individuals with useful information or decision-making powers. Foreign intelligence services exploit the desires of some individuals to feel important, to secure financial gain or their lack of self-reflection. It is important to spread awareness about the methods employed by foreign intelligence services among both junior and senior state representatives. This awareness includes e.g., also the need for caution when communicating with problematic individuals as just meeting them or discussing seemingly harmless topics can be easily abused. Considerable caution must be exercised when communicating with foreigners, whose business activities are linked to power interests of foreign states, especially to the activities of foreign intelligence services (e.g. Russian or Chinese).

The state faces a number of threats regarding the enforcement of state ownership rights. Enforcing state interests is difficult especially in joint-stock companies. The oversight system sufficient for the private sector has serious deficiencies in the state sector. There are a number of cases especially in the energy industry, in which a company's management effectively controls the supervisory board. Such supervisory boards do not fulfill their main function and the state as a

shareholder does not have an effective supervisory tool in the periods between shareholders' meetings. In such cases, state representatives do not sufficiently represent the interests of the state. The question of what leads to such failures in individual cases remains to be answered; however, it is clear that when a company's management controls the supervisory board the state's interests are not sufficiently protected.

Some state representatives were not willing to adopt necessary measures in the required time frame and take responsibility for these measures when making key economic decisions. Preference was given to safe solutions based solely on financial aspects without regard to important non-financial aspects such as energy security, status on the market or the good name. This attitude is often the result of fearing criminal or other sanctions for causing potential financial losses. The problem is that the loss or damage to non-tangible assets, which often have a higher value than the potential financial losses, is not sanctioned.

Activities not respecting economic competition pose a considerable threat to major economic interests. In 2015, the BIS detected efforts of bidders to enter into collusive agreements regarding public contracts for the construction of road and rail infrastructure or environmental contracts. This had a considerable negative influence on fair competition and led to an increase in contract prices. However, contracting authorities often have limited options of countering such collusive agreements. Therefore, the question is, whether the state has efficient tools (e.g. legislative or institutional) for addressing such issues. Moreover, invitations to public tenders also suffered from deficiencies. The contracting authorities often circumvented certain provisions of the Act on Public Contracts. Furthermore, some contracting authorities do not have sufficient capacity for the independent (i.e. objective) formulation of internal regulations and are not able to administer the whole process themselves.

As in previous years, the BIS detected illegitimate lobbying efforts regarding the legislative process and public administration. The efforts often focused on regulations and decision-making concerning the energy and healthcare industry. These industries have characteristics creating favorable lobbying conditions - strong state regulation, large volume of public funds and strong private interest in using these funds. Illegitimate lobbying efforts in the energy industry focused mainly on regulations providing for the subsidies and monitoring of some energy resources. Lobbyists in the healthcare industry focused on legislation providing for the remittance payments for pharmaceuticals and medical supplies, or on specific decisions made by regulatory bodies.

In 2015, the number of cases, in which companies with Russian capital did not follow the rules and violated especially tax and regulatory regulations and contract conditions, increased. The reason for this is the link of Russian capital to the "grey zone" of the legal system. If Russian parent companies or legal persons had financial problems, this led to higher tendencies to circumvent legal and contract conditions. In 2015, such cases were newly identified in companies, which are partly owned or directly controlled by Russian state administration.

## **2.2. Organized Crime**

### **Dysfunction in public administration**

Dysfunction in public administration is one of the main consequences of modern organized crime. In 2015, the BIS detected a number of cases of central and regional dysfunction.

Civil servants and individuals holding public posts with insufficient responsibility for their decisions are the main reason for dysfunction in public administration. In some cases, these individuals had no responsibility whatsoever. Often, unfavorable contracts were signed and public contracts were awarded to companies with an opaque ownership structure or without inviting a public tender. This led to the poor management of public funds; however, no criminal offences were committed and it was difficult to establish who is at fault. The responsibility of individuals often dissolved during the approval process by shifting from one individual to another without a clear definition of the role each stakeholder is to play in the final decision.

Dysfunction in public administration harming the interests of the Czech Republic and the EU was caused not only by negligence but also by intentional actions of individuals holding public or local administration posts, who had profit-seeking interests. These interests were advanced by illegitimate lobbying activities or by motivating public administration representatives by employing almost corrupt practices. Civil servants were motivated by both financial and other incentives.

The non-effective allocation of public funds presented as the protection of public interests was also a frequent manifestation of the dysfunction in public administration. In several cases, public interest (defined as total benefit to society) was an excuse for a broader or lax interpretation of established regulations governing the responsible management of public funds.

This led to the diversion of public funds to private parties. This had not only a significant economic impact on public budgets, but also weakened the effectiveness and credibility of public administration bodies. This would not have occurred, if the existing regulations were observed.

#### **Legislative changes related to limiting the opportunities of organized crime**

In November 2015, the Chamber of Deputies passed the Act on the Registry of Contracts - a key piece of legislation, which could improve the management of public assets and limit negative phenomena contributing to the dysfunction in public administration. This Act is a step forward in fighting modern organized crime.

As in 2014, the BIS focused on the amendment to the Civil Service Act. In 2015, the BIS focused on security threats linked to the gradual filling of senior civil service posts.

Furthermore, comprehensive measures regulating the oversight of financial management performed by municipalities were of interest to the BIS in 2015. The BIS focused especially on legislative measures linked to long-term problems regarding the management of public funds performed by municipalities. In individual cases, the financial impact of non-effective management seemed small; however, in recent years this dysfunction has been one of the major economic threats faced by the Czech Republic. There are several reasons for this. One reason is that the volume of devolved funds is growing. A further reason is that effective oversight mechanisms are already in place on the central level and the public oversight of management performed by state bodies is increasing.

In 2015, the BIS pointed out a significant drawback in the Act on the Management and Oversight of Public Funds - the exemption to the mandatory establishment of an internal audit body for municipalities with less than 15 000 inhabitants regardless of the volume of assets and funds managed yearly by the municipality in question. This exemption can seriously weaken the aim of this Act - to introduce modern oversight mechanisms on the local and central level of public administration.

The BIS repeatedly drew attention to public contracts, which were identified by law enforcement authorities, the Supreme Audit Office (in Czech: *Národní kontrolní úřad - NKÚ*) and other oversight bodies as cases of non-effective and purposeless wasting of public funds.

### Traditional organized crime

Organized criminal groups and traditional organized crime are not a priority and are only monitored by the BIS. Unlike the Police, the BIS does not have the means, powers and responsibilities to fight criminal groups. Furthermore, BIS findings cannot be used in criminal proceedings. Nevertheless, the BIS provides relevant information on criminal groups to other state bodies (usually to the Czech Police) with the remit to adopt relevant measures. In 2015, the BIS focused on the organized crime of groups involved in organized economic crime - i.e. the sale of untaxed goods - and of groups with a growing share in the drug trade.

### Migration

Since the second quarter of 2014, Europe has been facing a large migration wave from the Middle East, Sub-Saharan Africa and Maghreb. In 2015, more than a million refugees arrived in Europe. Their arrival had a negative impact on public order and on security and administrative procedures both in countries along the main migration routes and in destination countries. The Czech Republic is located in a heavily transited area of Central Europe and is faced by the same migration threats as France, Belgium and Germany. Nevertheless, due to the course of the migrant wave and its impact on the Czech Republic in 2015 the danger of these threats materializing is lower in the Czech Republic than in other countries.

The Czech Republic belongs to less popular transit and destination countries. The most serious migrant threats are not directly linked to the current migration wave but to its middle- and long-term impacts on Europe. These threats are mainly linked to the fact that it is virtually impossible to integrate a large number of foreigners from a different cultural environment into European society. This leads to the creation of enclosed communities with a possibly hostile attitude to European culture. These communities can serve as ideological or logistical havens for various criminal activities.

There were no international smuggling networks organizing the transit of migrants in the Czech Republic. Europol identified criminal groups organizing the transit of migrants between certain European countries; however, only individuals or small criminal groups offering limited transport and services to refugees were detected in the Czech Republic. The majority of migrants were transported to destination countries by public transport organized by individual states or they travelled individually with the help of their relatives, close associates or by individuals, who started a profitable business on providing services to migrants.

A pressing issue was the exploitation of the fear of foreigners leading to unease and concerns in society. This atmosphere of doubt created by the uncertainty whether other states are able to cope with migration, fueled extremist and populist political parties, led to the radicalization of the political environment and to rising popularity of extremist parties.

In 2015, new migration routes did not transit the Czech Republic. Czech authorities have been strictly conducting border checks, following registration procedures and upholding the rule that migrants not applying for asylum in the Czech Republic are regarded illegal migrants. This has significantly reduced the number of foreigners transiting via the Czech Republic. However, migrant

control procedures have certain limitations. One of the reasons is the fact that a number of migrants have (or are likely to have) travel documents, which were issued albeit officially on territory in source countries of migration controlled by extremists. Many migrants also use stolen or changed travel documents. Moreover, Czech authorities do not have a reliable official partner body in source countries of migration, which could help in screening the validity of information provided by the migrants and their travel documents and provide credible relevant information. A further security threat is the threat of transferring problems and conflicts from source to destination and transit countries affected by the migration wave.

### 2.3. Counterintelligence Activities

In 2015, Chinese and Russian intelligence services were the most active in the Czech Republic.

Chinese diplomatic, intelligence and economic entities focused on drawing on their success from 2014 and actively worked on extending and maintaining Chinese influence in Czech politics and economy.

In 2015, Russian activities focused on the information war regarding the Ukrainian and Syrian conflicts and on political, scientific, technical and economic espionage (especially efforts to exploit duped Czech individuals to gain access to Czech and European subsidies).

In 2015, the BIS did not identify any significant activities of intelligence services of other former Soviet Union countries or of partner intelligence services.

As in previous years, Russian intelligence services were the most active foreign intelligence services in the Czech Republic. A large number of Russian intelligence officers were active under diplomatic cover of the Russian Embassy. The Russian Embassy has much more employees than Embassies of other states (including the US and China). Intelligence officers under diplomatic cover were active also at the Embassies of other states; however, the number of Russian intelligence officials was much higher. Unlike intelligence officials of partner states, Russian (and some other) intelligence officers did not declare their status to the BIS. Such clandestine behavior concealing the affiliation to an intelligence services clearly signals activities threatening the security and other interests of the Czech Republic.

Regardless of the ongoing Ukrainian crisis and tense Russia-EU/NATO relations, Russia focused on activities aimed at maintaining and strengthening Russian positions and outlooks in Czech power engineering. Furthermore, Russian economic, scientific and technological espionage continued in 2015 in the Czech Republic.

In relation to the Ukrainian and Syrian conflicts Russia focused on influence and information operations as part of its non-linear (hybrid, ambiguous, irregular, non-conventional) warfare<sup>1</sup>.

---

<sup>1</sup> Non-linear warfare combines the use of force (kinetic elements) with non-military (non-kinetic elements) means of warfare (cyber-operations, economy, or politics); all of this is linked to powerful information warfare supported by ideology. Non-linear warfare takes place below the enemy's reaction threshold creating uncertainty about the legitimacy or appropriateness of a potential military response. Propaganda is a form of communication, an intentional effort to influence perception, manipulate facts and change behavior in order to achieve the goals of the propagandist. Propaganda (disinformation, deception) must be assessed with regard to



In 2015, Russian information operations in the Czech Republic focused especially on:

- weakening the strength of Czech media (covert infiltration of Czech media and the Internet, massive production of Russian propaganda and disinformation controlled by the state);
- strengthening the information resistance of the Russian audience (prefabricated disinformation from Czech sources for the Russian audience);
- exerting influence on the perceptions and thoughts of the Czech audience, weakening society's will for resistance or confrontation (information and disinformation overload of the audience, relativization of truth and objectivity, promoting the motto "everyone is lying");
- creating or promoting inter-societal and inter-political tensions in the Czech Republic (foundation of puppet organizations, covert and open support of populist or extremist subjects);
- disrupting the coherence and readiness of NATO and the EU (attempts to disrupt Czech-Polish relations, disinformation and alarming rumors defaming the US and NATO, disinformation creating a virtual threat of a war with Russia);
- damaging the reputation of Ukraine and isolating the country internationally (involving Czech citizens and organizations in influence operations covertly led in Ukraine or against it by Russia).

The above-mentioned activities pose a threat to the Czech Republic, EU and NATO not only in relation to the Ukrainian and Syrian conflicts. The infrastructure created for achieving these goals will not disappear with the end of the two conflicts. It can be used to destabilize or manipulate Czech society or political environment at any time, if Russia wishes to do so.

In 2015, Chinese military intelligence was the most prominent Chinese intelligence service in the Czech Republic. Its activities were supported by a specific Chinese intelligence organization - the International Liaison Department of the Communist Party of China. This agency falls under the Central Committee of the Chinese Communist Party and focuses on international relations and intelligence activities. In 2015, Chinese diplomatic, business and intelligence efforts drew on successes achieved in 2014 and actively worked on extending and maintaining Chinese influence in Czech politics and state structures.

Due to the worsening situation in the Middle East and the prominent role of Iran in the region, the BIS focused also on Iranian intelligence services. Regardless of Western efforts and international expectations, Iran upheld its decided attitude toward the West. The process of easing international sanctions and US efforts to improve international relations did not convince Iran to change its security and foreign policies. As in previous years, Iranian intelligence services focused e.g. on politics and economy.

---

the goal of the propagandist - the foreign power - and in the broader context of information and non-linear warfare. Propaganda is a neutral term, only a tool, which can have both beneficial and detrimental effects.

## 2.4. Protection of the Constitutionality and the of the Democratic Foundations of the Czech Republic

In 2015, the BIS did not identify any activities posing a specific direct threat to the democratic foundations of the Czech Republic from the perspective of an intelligence service. Extremists tried to address the broader public and secure public support for their views. A more serious new trend is the ability of extremists to overcome disagreements, personal and ideological differences and cooperate in certain cases.

### Anti-immigration and anti-Muslim activities

In 2015, the BIS focused on the migration wave to Europe and on its potential impacts on Czech society, especially in relation to the activities of individuals, who spread xenophobia, racism and other forms of intolerance. Immigration was a topic not only for extremists. The Czech public started perceiving it as a security threat. This led to an increase in activism and a number of public events took place.

A wide range of persons and groups held anti-immigration stances: right-wing extremists, various populist and other groups, which cannot be labeled as extremist by default. Representatives of these groups adopted an ambiguous attitude towards right-wing extremists. On the one hand, they tried to distance themselves from right-wing extremists in order to avoid being labeled as extremists; on the other hand, some of their statements were similar to right-wing extremist rhetoric.

Furthermore, also individuals wishing to legally express their anti-immigration stance took part in anti-immigration events. Even though they distanced themselves from cooperation with extremist groups (at least in the beginning), their events attracted various radicals or extremists. Therefore, it became difficult for the unformed public to differentiate between non-extremist and extremist groups.

Gradually, differences between individual anti-immigration groups started to fade and some groups intentionally started cooperating.

Anti-immigration attitudes were adopted also by individuals, who did not take part in public demonstrations, but expressed their anti-immigration stances online (especially on social media). Even though the majority of such individuals were not right-wing extremist sympathizers, a number of their statements could be perceived as extremist.

Some activities of individuals opposing anti-immigration demonstrations also posed a security threat. The reason is that not only individuals wishing to legally express their support for migrants, but also various left-wing extremists, who primarily tried to heighten tensions and provoke conflict, attended these events. A number of supporters of migration were willing to tolerate more radical stances and activities of left-wing extremists with the view of fighting for a common goal; however, left-wing extremists often employ the same undemocratic methods as right-wings extremists, who are criticized by the left-wing extremist scene for this behavior.

Some supporters of migration employing a manipulative or biased rhetoric and refusing to accept any criticism or a different opinion on the migration wave also posed a certain threat. In extreme cases, they threatened or assaulted their ideological opponents. Nevertheless, the lack of respect for the right to a different opinion and freedom of speech was characteristic of both parties - those opposing and those supporting migration.

The whole public debate about refugees (Islam in general) was characterized by prejudice, insufficient knowledge, ignorance, and shallow and biased knowledge / interpretation of basic historical, religious, social and cultural facts.

### Right-wing extremism

At the beginning of 2015, the situation on the right-wing extremist scene was similar to previous years. The scene remained fragmented, focused on itself and its internal problems. Even though right-wing extremists started expressing anti-immigration stances (e.g. in relation to the January attacks in France), they were not yet able to overcome disagreements in order to cooperate.

However, with the ongoing migration crisis two following trends were identified on the right-wing extremist scene:

1. Right-wing extremists, who previously refused to cooperate due to ideological or personal reasons and organized all anti-immigration demonstrations separately, started supporting each other. Growing public interest in migration led to increasing willingness to cooperate on organizing anti-immigration protests. The largest anti-immigration demonstration took place in November in front of the Cabinet Office, which brought together protestors attending several separate events. The police took action against several participants who refused to leave the site after the protest ended.
2. Extremists started establishing contacts that were more intensive or started cooperating with non-extremist anti-immigration groups - e.g. right-wing extremists attended events held by anti-immigration activists, together they organized protests, in several sporadic cases, friendly contacts were established.

Even though anti-immigration rhetoric increased significantly and anti-Islam and anti-immigration stances were the primary topic for all right-wing extremist groups, no serious attacks related to this matter took place. Only several offences occurred - e.g. right-wing extremists poured pig blood on a halal shop.

Compared to previous years, 2015 saw a major decrease in anti-Roma activities. No larger anti-Roma demonstrations took place and relations between the Czech majority and the Roma minority were normalized.

Some right-wing extremists held pro-Russian stances, which they actively expressed by publishing online articles and holding several events in order to attract the attention of the media. Pro-Russian stances were expressed also by some entities, which have not done so in the past. Right-wing extremists showed minimal interest in the situation in Ukraine. Their activities related to the situation in Ukraine were insignificant and did not change the Czech right-wing extremist scene. Ties established between Czech and Ukrainian right-wing extremists were based on personal contacts between individuals and did not pose a threat to the security of the Czech Republic.

Right-wing extremists showed some interest in protesting against the American military convoy travelling via the Czech Republic from March 29 to April 1 2015. The media paid considerable attention to the event and a number of right-wing extremist groups aimed to capitalize on that. However, the public largely ignored these activities of right-wing extremists.

Right-wing events accompanied by music were held. These concerts were usually not openly right-wing extremist. They became a social event and their ideological aspect faded. Attending

concerts abroad, especially in Slovakia, was still popular. Czech bands also performed several concerts abroad.

In 2015, cooperation among Czech and foreign right-wing extremists (especially from Germany, Slovakia, Poland, Austria, Italy and France) was based on contacts between individuals. Communication between Czech and foreign extremists was quite frequent and inspirational for Czech extremists.

The Internet played a significant role in promoting right-wing extremism and in enabling communication between individual groups. The role of Facebook was growing and this social media site became more prominent than standard websites of individual groups.

### Left-wing extremism

Left-wing extremists focused mainly on the European migrant crisis. To express their support for migrants they attended demonstrations aiming to block protests held by anti-immigration protestors represented not only by right-wing extremists.

These events were often characterized by violations of public order and the Czech Police had to intervene. The growing number of anti-immigration demonstrations led to an increased number of counterdemonstrations and to increased radicalism of left-wing extremists, who verbally attacked and provoked their ideological opponents. In several cases, left-wing extremists threw eggs at speakers and participants of anti-immigration demonstrations. In the second half of 2015, more dangerous objects were thrown at anti-immigration protestors.

Militant anarchist-autonomous groups conducted further arson attacks targeting police vehicles (the police is seen as a representative of state repression) and the vehicles belonging to the owner of the Prague restaurant *Řízkárna* (for allegedly exploiting his employees). The majority of the attacks were a reaction to the police operation *Fénix*, which took place on April 28, 2015 and which led to the arrest of individuals suspected of taking part in the activities of the Revolutionary Cells Network (in Czech: *Síť revolučních buněk – SRB*) in 2014. This police operation also led to the mobilization of moderate anarchist-autonomous groups, which held several protests and benefit concerts in the period from May to September 2015 in order to express solidarity with the defendants.

Sympathizers of anarchist-autonomous groups leading an alternative lifestyle focused on squatting. They held several smaller demonstrations supporting the Cibulka squat that was cleared by the police. Squatters also newly occupied an abandoned building in Prague. Various social community centers often served as squats and different cultural events took place in these centers - lectures, benefit concerts, author readings, workshops on attending demonstrations, solidarity events expressing support e.g. for the anarchists detained in the police operation *Fénix*.

The Marxist-Leninist spectrum of the left-wing extremist scene continued to stagnate. Marxist-Leninist groups were active mostly on the Internet and expressed their extremist views only in online articles. They held only a few events and attended rallies organized by other left-wing groups.

### Non-state paramilitarism

In 2015, initiatives to establish street patrols and various paramilitary groups were detected. These efforts were initiated not only by right-wing extremists but also by individuals without an ideological background. The activities of such groups were linked to certain covert security threats.

However, in 2015, these groups did not pose a direct threat to the democratic foundations of the Czech Republic.

## 2.5. Terrorism

National and international cooperation, mutual exchange of information and trust between intelligence services and other security authorities of the democratic world are integral for the fight against international terrorism. Cooperation regarding the fight against terrorism is highly effective and functional; however, the unfortunate choice of words sometimes creates an inaccurate notion of this cooperation, its quality and results. In recent years, the BIS has been exchanging tens of thousands of requests for information and responses to these requests with its national and international partners. Security authorities (including the BIS) exchange information and screen natural and legal persons for the purposes of projects falling under the remit of other state bodies (e.g. the Ministry of the Interior or the Foreign Ministry). The goal is to support the state and the state's efforts to protect the interests of the Czech Republic and its citizens and to limit or completely eradicate security threats.

The dramatic developments in 2015 led to the worsening of the security situation in EU and Schengen Member States, including the Czech Republic. The Paris terrorist attacks and all related events became the main impulse for the work of all cooperating intelligence services. The BIS worked with its partner services on mapping the travels of confirmed, suspected and potential attackers. The screening of the names of thousands of extremists revealed that in 2015 some of them transited via the Czech Republic on their travels between the Middle East and Western Europe. Set in a wider context it is clear that a potential threat of a terrorist attack conducted by Islamist jihadists linked to the so-called Islamic State (IS) or to the Al-Nusra Front (the Syrian branch of al-Qaeda) is present also in the Czech Republic.

Even though the Islamic State has lost territory and fighters, the group managed to conduct several terrorist attacks in Europe and in the Middle East in 2015 (e.g. in Lebanon, Turkey, Egypt). Furthermore, the Islamic State intensified its propaganda aiming to radicalize and recruit new fighters. Therefore, the BIS focused on two groups of individuals potentially posing a threat:

1. The BIS monitored individuals, who expressed support for the ideology or activities of the Islamic State or a similar group. The BIS identified only several supporters among individuals targeted by the Islamic State (the younger generation of Muslims and covert). In the majority of cases, the views they expressed were a symptom of mental instability, frustration or a disorder. These individuals did not have ties to Islamist groups or to any local Muslim communities. With a few exceptions, Muslims living in the Czech Republic have publicly denounced the activities of the Islamic State.
2. The BIS obtained information on individuals travelling from the Czech Republic with the intent to join terrorist groups in Syria, especially the Islamic State. In total, seven individuals from the Muslim world, who shortly stayed in the Czech Republic, were identified. The return of these individuals to the EU would pose a serious security threat in relation to their involvement in terrorist attacks. The BIS shared obtained information with national and international partners.

The activities of the Islamic State in the Middle East and the above-mentioned terrorist attacks in Europe triggered numerous reactions. Adverse reactions were produced mainly by individuals with an anti-Muslim sentiment, who do not differentiate between Islamist terrorism and

Islam. Muslims, who are not official representatives of the local Muslim community and its organizations and do not represent the community's opinions, managed to attract more media attention. This led to heightened tensions between the Czech majority and the Muslim community. Some manifestations of these tensions - verbal attacks, insults of fellow Muslim citizens - can become a relevant radicalization factor.

The refugee crisis was a major development in 2015 related to terrorism. Refugees from Syria, Iraq and Afghanistan were joined by migrants from Africa. The Islamic State took advantage of the migration wave and sent two Syrians to the EU with the goal of conducting suicide terrorist attacks in Paris. This confirmed the fears of the intelligence community, which warned about terrorists taking advantage of the migration wave to reach the Schengen Area. Therefore, the BIS focused on identifying other problematic individuals among migrants from the Middle East.

The BIS identified migrants from the Muslim world, who abused the European asylum and immigration policy provided for in the Czech Republic by Act No. 326/1999, on the Residence of Foreign Nationals in the Czech Republic. Provisions on long-term residence permits for the purpose of family reunification, studies or business have been subject to abuse. Foreigners violating the conditions for obtaining a long-term residence permit in the Czech Republic intentionally provide false information and mislead Czech authorities. The process of issuing and revoking residence permits for foreign nationals in the Czech Republic is limited by current legislation in that it does not provide for an appropriate means of taking into account intelligence provided by intelligence services and of protecting intelligence sources.

The majority of these individuals did not pose a direct security threat; however, potential security threats were identified in relation to some of them, e.g. several of these individuals supported Islamic State Ideology.

## 2.6. Proliferation of Weapons of Mass Destruction

### Proliferation of weapons of mass destruction

The Czech Republic is a member of several International Control Regimes<sup>2</sup> committed to fighting the proliferation of weapons of mass destruction and their carriers (WMD).

In the Czech Republic, foreign trade in dual-use goods, military equipment, weapons and explosives is governed by legal regulations. Nuclear, chemical and biological (bacteriological and toxin) WMDs are completely excluded from trade.

The BIS focused on the circumvention or violation of Czech Republic's international obligations linked to international sanctions imposed on individual countries or entities. Information on specific incidents, phenomena or trends provided by the BIS to entitled addressees strives to minimize risks related to the international trade with controlled goods.

---

<sup>2</sup> The Australia Group (AG), the Missile Technology Control Regime (MTCR) reinforced by the Hague Code of Conduct (HCoC), the Nuclear Suppliers Group (NSG), the Zangger Committee (ZC), the 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).

North Korea and Iran - the countries posing the gravest proliferation threats - continued to seek engineering devices, special materials, technologies or know-how falling under the category of internationally controlled goods. International sanctions prevented direct exports of such goods to North Korea and Iran and the transfer of payments for such trade deals with the two countries. The BIS focused on obtaining information about the role of various front companies in planning complicated trade routes via third countries. Complicated trade routes are accompanied by payments, which aim to prevent the identification of the routes and of the companies involved. China is the main re-export country for goods heading to North Korea. Companies from China, the United Arab Emirates and Turkey were involved in the re-export of goods to Iran.

Those interested in trading with Iran waited for the sanction changes resulting from the political agreement between the US, UK, France, Russia, China, Germany, and the EU (E3/EU+3) with Iran in July 2015 known as the Joint Comprehensive plan of Action (JCPOA), an agreement on Iran's nuclear program. The JCPOA lifted certain financial sanctions; however, sanctions on conventional weapons and rocket program remain in place.

Trade with dual-use goods, weapons and military equipment continued even though sanctions against Russia were in place. Some businesspersons in the Czech Republic took advantage of the exemptions applying to contracts concluded before the sanctions entered into force in August 2014.

In relation to the general threat of terrorist attacks in Europe and in reaction to the attacks in France, the BIS focused on inadequately deactivated weapons not subject to further controls. Such weapons were transferred to the Czech Republic from abroad, where they were sold also by online stores. The Czech Act on Firearms stipulates that a deactivated weapon is a weapon subject to irreversible modifications that cannot be used for shooting. However, not only were firearms inadequately deactivated abroad, but they were also modified and transformed into expansion weapons. The transformation into expansion weapons excluded the use of rifle ammunition or shotgun shells. However, deactivated or expansion weapons could quite easily be reactivated.

Even though it has been confirmed that the threat of abusing weapons or other controlled items still exists, lobbyists campaign for simplifying and easing regulations on the trade with these goods. Specific cases, in which controlled items were abused abroad, are a strong argument for strictly enforcing relevant legal regulations and control mechanisms.

## 2.7. Cybersecurity

### Cybersecurity

As in previous years, the BIS informed the Czech Ministry of Foreign Affairs about attempts to exploit Visapoint - an information system enabling foreigners to schedule an appointment at Czech embassies online. Visapoint has been a long-term target of cyberattacks. Individuals and groups have been using automated tools to override the registration procedure in order to secure financial benefit by selling the occupied appointment dates. These activities significantly affect the good name of the Foreign Ministry and the Czech Republic.

The BIS also investigated activities, which seemed as DDos attacks aimed at the Visapoint system. However, the investigation revealed that the IP addresses that were allegedly used for the attacks are used for automated registrations in the systems.

In relation to the investigation of suspicious registrations for appointments, the BIS learned that in 2014 several registrations were made by the user of an e-mail address and telephone number belonging to a foreign employee of a Czech embassy. It is highly likely that the registrations were made directly by this employee. It is possible he took advantage of his knowledge of internal systems and processes related to issuing visas. He could have also made use of his connections at the embassy, his knowledge of how the system works, of information available in embassy information systems or of information available to the Ministry in order to facilitate or secure the issuance of a certain visa. This sphere is also vulnerable to the threat of espionage or illegitimate cooperation with a foreign power.

In 2015, the BIS obtained information about insufficient security of some municipal radio systems. The technology used for these systems does not meet the security standards employed by developed countries. Therefore, it does not provide sufficient security of communication and data transfers between individual stations and sufficient protection against abuse.

The BIS informed entitled addressees about potential exploitation of vulnerabilities of online applications and cloud services related to systems, where one server is used to run several different online applications accessed by logging in. These vulnerabilities apply also to cloud services with the same problem, i.e. one server is used to simultaneously run several different services or applications. There are probably more than a million applications with these vulnerabilities only in the Czech Republic. State bodies usually do not use shared application hosting services; therefore, it can be presumed, that these vulnerabilities apply mainly to commercial entities. Nevertheless, it cannot be ruled out that user profiles of those state bodies, which use these services, could be attacked.

Dozens of small companies that cannot afford to run their own server for their own online applications (e.g. the majority of online shops) can become the target of a cyberattack. Data on clients can be stolen, false orders can be placed, the functionality of individual applications can be damaged, or unfair competition can take place, etc. Some entities can become “accidental” targets of a cyberattack only because they use the same hosting or cloud service as the targeted victim. The threat of espionage is greatly underestimated. Many Czech companies are not aware of this threat and do not have sufficient information on the dangers they face.

### **State-sponsored cyber-espionage campaigns**

Long-term state-sponsored cyber-espionage campaigns organized either by state bodies (representatives of the state) or by entities sponsored by the state have been taking place all over the world. It is highly likely that increasing digitalization of public services will lead to a growing number of state-sponsored cyber-espionage campaigns. The BIS has detected this trend in its own investigations and in information provided by foreign partners.

Such campaigns focus on obtaining political, military, diplomatic, scientific, technical, industry and power engineering information. The stolen information can be used to serve the attacker’s goals (political, scientific, or technological), to discredit certain individuals or states, to spread disinformation or to carry out blackmail.

However, data or classified information is not the main target of cyber-espionage attacks. The attackers focus on stealing personal data and ICT logins and on accessing the electronic



communication of politically or otherwise prominent individuals. This data is used for further sophisticated attacks employing social engineering methods.

In 2015, the BIs obtained information on possible Czech victims of a new wave of a Russian cyber-espionage campaign. Two Czech ministries were on the list of potential targets. The attackers targeted mainly routers, which they used to re-direct network traffic of interest to IP addresses under their control.

The investigation of these cyber-espionage attacks is ongoing and is one of the priorities of the BIS in securing cybersecurity.

In 2015, the BIS informed entitled addressees several times about attacks that were part of specific cyber-espionage campaigns. Due to intensive and effective cooperation, the BIS managed to obtain a considerable amount of data enabling the development of detection statistics, which could be used to detect potentially compromised information and communication systems or prevent such an attack from taking place.

The attackers often used spear phishing attacks employing social engineering methods and “watering hole attacks”.

The number and sophistication of cyber-espionage campaigns is growing. Older cyber-espionage campaigns are conducted even after their detection or they are re-sold. This is probably the reason, why the number of states able to lead their own cyber-espionage campaigns is not changing. Russia and China pose the gravest threat to the Czech Republic as far as state-led or state-sponsored cyber-espionage campaigns are concerned.

### **3. Protection of Classified Information**

#### **3.1. Administrative Security**

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

#### **3.2. Security of Information and Communication Systems**

All BIS information systems processing classified information have a valid National Security Authority certificate. New security software has been installed that can be used in handling various security incidents.

As far as the cryptographic protection of classified information is concerned, no serious incidents or problems related to cryptographic devices occurred in the BIS.

#### **3.3. Physical Security**

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

Documentation on BIS offices and buildings was regularly updated. Due to the relocation of some workplaces, relevant documentation was updated 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 Intelligence Services of the Czech Republic and with other State Authorities

### 4.1. Cooperation with Intelligence Services of the Czech Republic

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

The BIS closely cooperated with the Office for Foreign Relations and Information and with Military Intelligence on fighting WMD proliferation and the illegal trade in military equipment.

In 2015, the BIS cooperated on fighting terrorism with other intelligence services of the Czech Republic – either individually or working together in the Joint Intelligence Group of the Cabinet Office of the Czech Republic.

Furthermore, the BIS regularly cooperated with Czech intelligence services on investigations requested by foreign partner intelligence services.

### 4.2. Cooperation with the Police of the Czech Republic

In 2015, the BIS played an active role in regular meetings of the National Contact Point for Terrorism (in Czech: *Národní kontaktní bod pro terorismus – NKBT*) falling under the remit of the Unit Combating Organized Crime (in Czech: *Útvar pro odhalování organizovaného zločinu*) of the Criminal Police and Investigation Service (in Czech: *Služba kriminální policie a vyšetřování*).

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

Effective bilateral cooperation related to individual cases took place with relevant police units, especially with specialized units.

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

The BIS and the Unit Combating Corruption and Financial Crimes of the Criminal Police and Investigation Service discussed dysfunctional public and local administration, organized crime infiltrating public administration, and individual persons and advocacy groups of interest.

In 2015, the BIS continued to cooperate with the Police of the Czech Republic on issues regarding illegal trade and manipulation with military equipment, security equipment, guns, ammunition, explosives, hazardous materials, and on fighting WMD proliferation.

### 4.3. Cooperation with other State Authorities and Institutions

In 2015, the BIS worked closely with the National Security Authority on protecting classified information. Cooperation involved mainly the following investigations based on NBÚ requests: investigations pertaining to personal and industrial security and security clearance and security clearance investigations examining whether a natural or legal person holding a security eligibility certificate still meets the requirements for their issuance. Throughout the year, meetings regarding the cooperation on specific cases were held.

Furthermore, the BIS worked with the National Security Authority on enhancing cybersecurity by exchanging information on security incidents with the National Cyber Security Center (in Czech: *Národní centrum kybernetické bezpečnosti*), a part of the National Security Authority.

The BIS cooperated also with Czech custom authorities - the Directorate General of Customs (in Czech: *Generální ředitelství cel – GŘC*) and local customs directorates - on fighting WMD proliferation. The BIS provided these authorities with information on the threat of military equipment being re-exported from the Czech Republic to a sanctioned country.

Cooperation in the fight against WMD proliferation took place also with the Ministry of Foreign Affairs, the Ministry of Industry and Trade Licensing Administration, and with the State Office for Nuclear Safety (in Czech: *Státní úřad pro jadernou bezpečnost*) and its subordinate organizations.

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

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

The BIS cooperated also on projects of other state authorities (e.g. of 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 processed requests related to tens of thousands of natural and legal persons.

In 2015, an amendment of Act 49/1997, on Civil Aviation, came into force, which stipulates provisions regarding reliability certificates issued to legal persons by the Civil Aviation Authority. These screenings include a credibility assessment of the legal persons conducted by the Czech Police. In relation to this matter, the BIS processed several thousand requests.

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

In addition to providing and exchanging information, the BIS provides other state authorities with generalized findings and recommendations when commenting on various legislative and non-legislative documents. Furthermore, the BIS provides 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. The BIS is authorized by the Government to cooperate bilaterally with over a hundred of intelligence services. As far as multilateral cooperation in 2015 is concerned, the BIS was very active in several organizations, e.g. the Counter-Terrorist Group (CTG) or the NATO Civil Intelligence Command (CIC). In 2015, the BIS extended both bilateral and multilateral cooperation. In certain areas, the BIS had a substantial influence on the work of multilateral groups.

The BIS received more than 8 100 reports from its foreign partners and sent almost 1 500 documents. BIS representatives took part in several hundred international strategic and expert meetings.

The cooperation continued to focus mostly on the fight against terrorism, counter-intelligence and proliferation. The exchange of information related to extremism increased in relation to the migration wave marking the year 2015.

## 6. Oversight

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

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

Sections 14 to 16 of Act No. 153/1994 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. This body is not created by legislation; its establishment is dependent on a Chamber of Deputies Resolution. Direct parliamentary oversight of intelligence services as stipulated by Section 12 of Act No. 153/1994 is defined by separate legislation; therefore, the above-mentioned respective body for intelligence services acts to a certain extent as a means of parliamentary oversight of the Government.

The separate legislation mentioned in Section 12 of Act No. 153/1994 is the Act No. 154/1944, on the Security Information Service, as amended. Under Section 18 of the said Act, the responsibility for overseeing the activities of the BIS lies with the Chamber of Deputies, which sets up a special oversight body (the Standing Oversight Commission). Sections 19 and 20 of the said Act provide specifically for the powers of the Oversight Commission. Authorized members of the oversight body may, e.g., enter BIS buildings when accompanied by the BIS Director or by a BIS official designed by the Director for this purpose; or request due explanation from the BIS Director should they feel that the activities of the BIS illegally curb or harm the rights and freedoms of citizens. The Director of the BIS is obliged to provide legally defined information and documents to the Oversight Commission.

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

## 6.1. External Oversight

External oversight of the BIS is carried out by authorities and institutions with the legal right to oversee individual activities of the BIS. In 2015, 4 external audits were conducted - an audit of pension insurance, food hygiene and municipal hygiene. No deficiencies were found.

## 6.2. Internal Audit

In 2015, the internal audit group carried out 4 inspections focusing on: public procurement, the cultural and social needs fund, and on the implementation of recommendations approved by the Director of the BIS.

Other expert monitoring units of the BIS conducted 55 inspections. The controls focused on compliance with internal regulations regarding an economical and effective management of individual BIS departments. The inspections focused on the following areas:

- fulfillment of the budget; adherence to binding limits and the keeping of records; adherence to budget discipline, including adherence to principles of allocating money from the cultural and social needs fund;
- provision of material needs in organizational units and keeping material records;
- monitoring the technical condition of vehicles, required vehicle inspections, adherence to fuel consumption norms;
- monitoring the structural condition of buildings and their usage in accordance with their intended purpose; conducting prescribed inspections; adherence to principles of occupational safety and hygiene, fire protection, water management, and of ecology; monitoring energy consumption.
- the equipment of buildings with security technologies and the effective use of the installed technologies.

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

In compliance with Act No. 187/2006, on Sickness Insurance, the BIS carried out 10 inspections of persons temporarily unable to work. The inspections did not reveal any shortcomings.

Employees of the archive and of the control group carried out 50 archive inspections related to records management. The inspections focused mainly on establishing that no classified documents or their parts were missing, on meeting administrative requirements, and on the precision of keeping record entries.

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

As far as physical security and the consolidation of security documents are concerned, the following inspections were carried out: adherence to requirements for the storage of classified documents; inspections of installed security elements, including of objects and security lock systems.



## **7. Maintenance of Discipline; Handling Requests and Complaints**

The work of the BIS Inspection Department is based on internal regulations providing for the activities of inspection officials.

The BIS Inspection Department focuses on three main areas:

1. It acts as the BIS police authority in compliance with Section 12, Paragraph 2 of the Criminal Code in cases, in which a BIS official is suspected of having committed a crime;
2. It investigates cases, in which BIS officials are suspected of having committed disciplinary breaches or of conduct having the traits of a misdemeanor, and emergencies.
3. It processes complaints, notifications and suggestions submitted by BIS officials and by other entities.

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

In this area, the BIS Inspection Department focuses on traffic accidents involving Service officials (accidents both caused and not caused by BIS officials). The Inspection Department is responsible for findings that cannot be provided by the police but are important for a decision in the matter.

### **7.2. Investigations of Complaints and Notifications**

In 2015, the BIS Inspection Department investigated complaints, notifications and suggestions from BIS officials as well as other entities. No submission out of the 206 in total was declared a complaint. Compared to 2014, the number of notifications and suggestions increased by 62.2 %. In terms of content, reports made by citizens reflected society-wide developments in the Czech Republic and abroad.

## 8. Budget

The budget of the BIS in 2015 was stipulated by Act No. 345/2014 from December 10, 2014, on the State Budget of the Czech Republic for 2015.

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

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

Furthermore, a part of capital investment expenditures was allocated to information and communication technologies.

The budget reflects requirements on the protection of classified information provided for in Act No. 412/2005, on the Protection of Classified Information and on Security Clearance, especially in the areas of physical, administrative, and personnel security, and in the area of security of information and communications systems. The need to take these facts into consideration in the whole spectrum of activities of the BIS leads to many expenditures that do not occur in other organizational units of the state.

Funds were allocated also to the technical support of software and hardware products, to procurement and upgrades of technical equipment needed for obtaining, processing, analyzing and storing visual and audio documents.

Funds were provided also for the development, production and modification of technical equipment in order to keep up with technological development and due to poor choice on the market and the non-existence of needed solutions.

In 2015, the basic operational needs of the BIS were met. Certain projects considered key for the BIS were by funded from unused expenditure.

As far as personnel are concerned, the allocated funds led to a slight improvement. In 2015, funds were available for a 3 % increase in the number of occupied Service posts compared to 2014. However, due to the current situation on the market, the demanding recruitment process and the number of members leaving service, the increased recruitment efforts did not lead to a 3 % increase in the number of occupied Service posts.

### Indicators of Budget Section 305 – Security Information Service in 2015 (thousands)

	Approved budget	Amended budget	Real data
Total revenues (CZK)	144 400	144 400	156 659
Total expenditure (CZK)	1 207 324	1 269 286	1 207 681

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