

# SECURITY INFORMATION SERVICE



Annual Report for 2020



**Annual Report  
of the Security Information Service  
for 2020**





## Table of Contents:

|            |   |    |
|------------|---|----|
|            | A Message from the Director General of the Security Information Service       | 5  |
| <b>1</b>   | Nature and Scope of Intelligence Activities                                   | 6  |
| <b>2</b>   | Intelligence Activities and Findings  | 8  |
| <b>2.1</b> | Impact of the COVID-19 Pandemic on Security                                   | 10 |
| <b>2.2</b> | Intelligence and Subversive Activities Targeting the Czech Republic           | 13 |
|            | Russia  | 14 |
|            | China   | 15 |
|            | Iran  | 16 |
|            | Cyberattacks  | 17 |
| <b>2.3</b> | National Economic Interests   | 19 |
| <b>2.4</b> | Violent and other Activities against Democratic Principles                    | 21 |
| <b>3</b>   | Protection of Classified Information, Security and Crisis Management          | 24 |
| <b>4</b>   | Cooperation with Czech Intelligence Services and with other State Authorities | 26 |
| <b>4.1</b> | Cooperation with Intelligence Services of the Czech Republic                  | 26 |
| <b>4.2</b> | Cooperation with the Police of the Czech Republic                             | 27 |
| <b>4.3</b> | Cooperation with other State Authorities and Institutions                     | 28 |
| <b>5</b>   | Cooperation with Intelligence Services of Foreign Powers                      | 31 |
| <b>6</b>   | Oversight   | 32 |
| <b>6.1</b> | Internal Oversight and Internal Audit   | 33 |
| <b>7</b>   | Maintenance of Discipline; Handling Requests and Complaints                   | 34 |
| <b>8</b>   | Budget  | 35 |





## A Message from the Director General of the Security Information Service

Dear Readers,

I have the pleasure of presenting to you the unclassified edition of the Annual Report on the Activities of the Security Information Service for 2020. In the past year, the whole of our country has experienced one of the most difficult periods in its modern history. I would like to use this opportunity to express my utmost admiration and gratitude towards all healthcare and emergency service workers and all the others who stood in the first line during the struggle against the COVID-19 pandemic.

Intelligence services, too, had to face the pandemic and its impacts. On one hand, almost all types of threats monitored by the BIS decreased; on the other hand, our work was affected by various health protection measures on everyday level. I would therefore like to use this opportunity to thank all my colleagues for having fulfilled their duty of protecting the security of the Czech Republic in defiance of the unfavourable circumstances. Despite restrictions caused by the pandemic, the BIS met with success in 2020 with regard to not only counter-intelligence but also the protection of national economic interests and counter-terrorism.

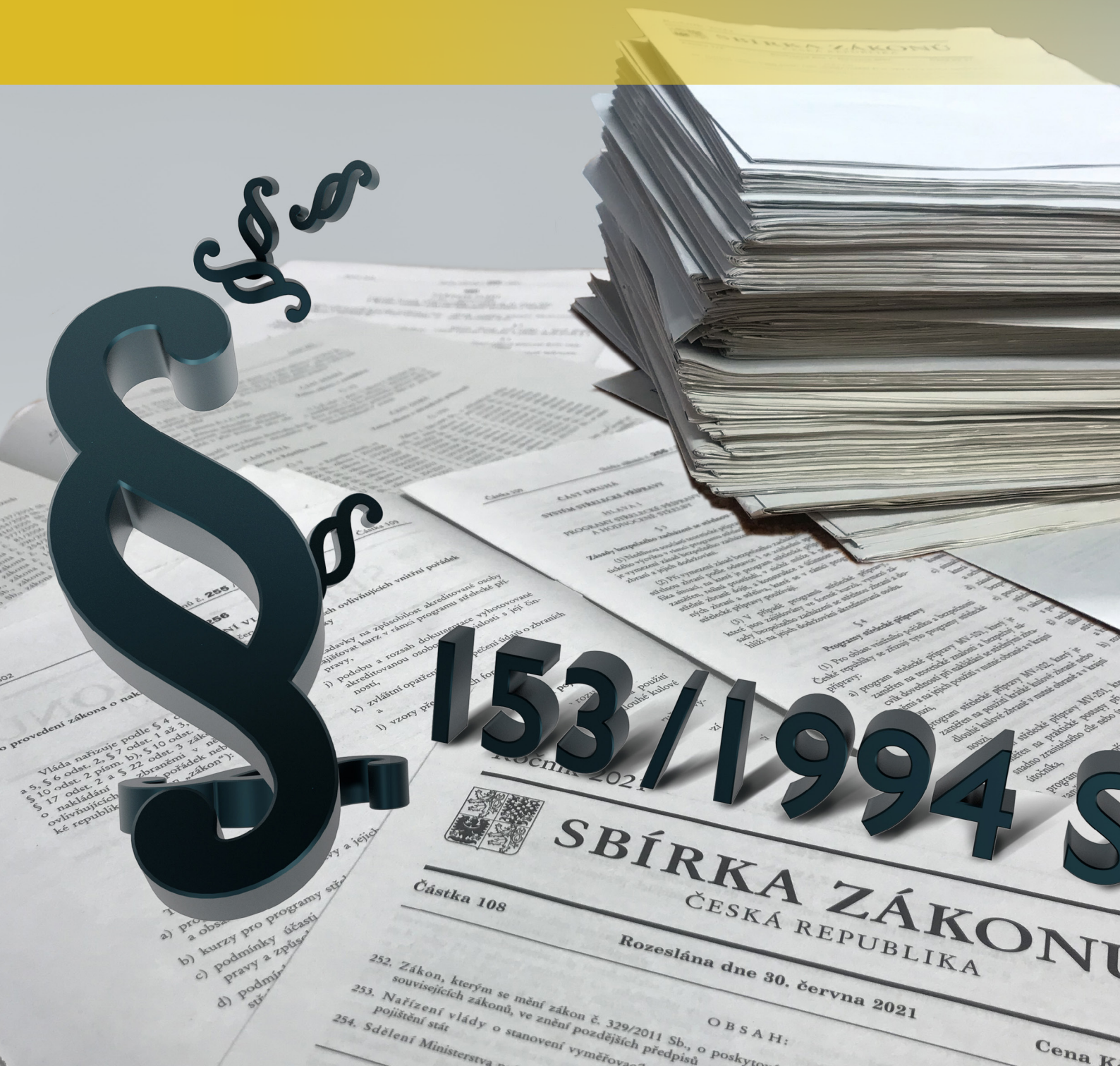
The unclassified Annual Report for 2020 has been conceived in a slightly different way than in previous years. The changes could hardly be described as dramatic, but we aimed to offer the general public as well as expert audiences a slightly different insight into the work of the main Czech intelligence service in an updated format.

As in previous years, I believe that the Annual Report will inspire a debate on whether intelligence services should publish unclassified reports. In the past, a few isolated voices expressed the view that by doing so, the Service ventures into politics. I insist on affirming my belief that the Annual Report is a tool, which allows every citizen to get an overview of the Service's tasks and consequently, to participate in supervising the Service's work. One of the predecessors to our Service used to be called the Office for the Protection of Constitution and Democracy and I am convinced that its name expressed perfectly what still constitutes our mission. Our task is to draw attention to threats to the fundamental democratic, security and economic principles of our country. When doing so, we abide by the applicable law and are determined to continue protecting the Czech Republic and its citizens in the future.

I sincerely wish that you find this year's Annual Report interesting and stay in good health.

Col. Ing. Michal Koudelka

# Nature and Scope of Intelligence Activities





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

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

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

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

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

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

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

# Intelligence Activities and Findings







The year 2020 was a special year not only from the point of view of intelligence. The COVID-19 pandemic can simply be described as the perfect black swan of intelligence operations.<sup>1</sup> Even though restrictive measures hindered the arrivals and travelling of agents and officers of foreign intelligence services in our territory, they also strongly interfered in the intelligence operations of the BIS. Nevertheless, despite the extensive anti-pandemic restrictions, the BIS successfully fulfilled its legal obligations all throughout the year and continuously informed entitled addressees about threats to national security interests. Last year, the BIS submitted almost 300 documents, several dozens more than the previous year, to the President and Government Ministers. A further 350 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.

The main intelligence topics of the past year as evaluated by the BIS were efforts to influence the preparations of a new nuclear source construction in Dukovany, cyberattacks of actors linked to foreign powers and disinformation activities which could weaken the democratic foundations of the rule of law. The BIS also secured crucial information regarding proliferation networks actors with links to the Czech Republic, individuals with radicalisation potential and activities of foreign intelligence services in our territory.

Last year was also marked by an intensive involvement of the BIS in the newly emerging structures of the national security system, which are aimed at sharing information and

experience in the area of hybrid threats. For the BIS, hybrid attacks do not represent a new or unknown phenomenon but another name for a coordinated combination of activities which fall under security threats and are of long-term interest to the BIS. A reaction to a coordinated approach of the attacker requires appropriate cooperation of individual bodies of the national security system, including intelligence services.

In 2020, too, the BIS worked on completing information about the subversive attack on the Vrbětice ammunition depots, which the security forces of the Czech Republic found was orchestrated by officers of the Russian intelligence services. Based on this finding, it is necessary to place all the intelligence which the BIS acquired in the given period into the context of the Czech Republic being attacked by a foreign state. This subversive act led not only to significant economic damage but also to the death of two Czech nationals and disrupted the lives of thousands of inhabitants of the municipalities in the immediate vicinity of the site.

In the coming period, the BIS expects that the main threats of increasing gravity for the security interests of the state will be activities which jeopardise the democratic foundations of the rule of law. Another topic which will grow in importance will be cyberspace security and the increasingly assertive behaviour of China, which manifests itself also in the Czech Republic. The danger of a lone-wolf terrorist attack will continue to represent an important challenge, especially given the growing role of the Internet in radicalisation of potential attackers and taking into account new trends in terrorism and migration in the security landscape, which has been reshaped by the withdrawal of allied forces from Afghanistan.

1 The term “black swan” designates a rare, unexpected event. It was popularised in 2011 by N. N. Taleb



# Impact of the COVID-19 Pandemic on Security



The COVID-19 pandemic hit the activities of intelligence services like it hit all other areas of human activity. However, no crisis brings only losses and discomfort, but also new opportunities and discoveries. The pandemic restrictions for instance showed that traditional diplomatic cover of foreign intelligence officers is of key importance especially in periods of crisis, as legal residency becomes irreplaceable at such times.

The coronavirus crisis also provoked a wave of negative reactions to anti-pandemic measures, which led to the formation of the so-called COVID-denial movement. This movement not only rejects governmental measures put in place to prevent the spreading of the infection, but it also questions the severity of the COVID-19 disease as such. It connected dissatisfied citizens with representatives of the Czech disinformation



scene, who also took part in organising some events. Within the scope of its authorities, the BIS focused on attempts to misuse these negative reactions to the anti-pandemic measures and instigate violence, organise deliberate spreading of false information and potentially apply or spread influence of foreign powers.

Due to the anti-pandemic measures put in place, associated disinformation and conspiracy theories found audience also among members of the public who normally avoid topics traditionally prone to manipulation. Even though disinformation and conspiracy theories affected wider population than usual, the COVID-denial movement was not successful in mobilising the general public. The low social impact was due, among other, to the mutual animosity of the movement's representatives, which meant that there was no unified organization or leading figure and that the whole COVID-denial scene fragmented.

For the past few years, the BIS has warned in its reports against increasing risks linked to the spreading of deceitful and manipulative claims in the society. The so-called alternative media present their own or adopted biased, manipulative or even deceitful content as an "alternative view" on current events. Even though those who spread disinformation pragmatically expand their scope of interest to any new topics which might arouse emotional reactions of the public, their long-term narratives relating to the Czech Republic have more or less stabilised. They include continuous critique of the political system and representation, membership of the EU and the NATO, critique of the functioning of these organisations and discrediting of general values of liberal democracy. The focus of such disinformation in terms of topics has therefore long been fully in line with the interests of Russia.

The persons most active in disseminating disinformation are often those highly motivated by their ideological beliefs, who

are traditionally inclined to sympathise with authoritarian powers or their representatives, and who are often persuaded that they are "educating" the society blinded by mainstream or official interpretations of the events. Some of them consider themselves to be modern dissidents suppressed by the majority society, but ironically, it is especially these individuals who knowingly or unknowingly contribute to the promotion of foreign powers' interests to the detriment of the strategic interests of the Czech Republic. Some of the individuals who create or spread disinformation are motivated by own economic profit which the spreading of disinformation brings (e.g. in the form of remuneration for advertisement or sponsorship of a related entity).

In 2020, the pressure on quality media, including public media, by the disinformation ecosystem further increased. Quality journalism continuously warns against content manipulation and disinformation, which logically makes it a target of verbal attacks and discrediting campaigns on the part of the so-called alternative media. Continuous disinformation pressure also contributes to the resignation of part of the society to the functioning of the state in its current constitutional form, which restricts the state's ability to communicate strategic topics to the affected part of the society and by extension eventually increases the vulnerability of the state and the society to influence operations of foreign powers.

The COVID-19 pandemic did not significantly influence the level of terrorist threat in the Czech Republic even though in some cases it contributed to the intensification of risk factors, such as financial difficulties and mental issues. At the same time, however, it temporarily hampered the logistics of global terrorist organisations, the movement of their members and opportunities for committing an act of terrorism in the Czech Republic. The moderate approach of the Czech Muslim community has been confirmed, apart from a few exceptions, by the responsible approach

of official Muslim organisations to following restrictive measures imposed by the state.

The pandemic significantly affected the functioning of the Czech Muslim community. The primary means of social contact among Muslims during the pandemic was the Internet, especially social networks and other communication platforms. These are often used to spread Islamist radicalisation and conspiracy theories, but the BIS did not acquire any information about any growing real risk of radicalisation of Czech Muslims via social networks.

Even though last year was marked by a significant increase in the use of information and communication technologies in everyday life, the BIS did not note any important changes in the techniques, means or methods used by cyber attackers. One of the most commonly used techniques was without doubt spear-phishing, which consists of sending emails with malicious attachments or links with the aim of infecting the device of the recipient. In the past year, there were cases of misusing compromised Czech mailboxes as well as efforts to attack Czech citizens or state institutions.

A second very common method of conducting a cyberattack were active attempts of attackers to find vulnerabilities in networks or systems operated or used by state and private entities. Scanning usually serves as the initial stage of a planned attack and helps the attacker to discover vulnerabilities which they could exploit to penetrate into the internal network.

A third type of attack was the so-called brute-force attack, which consists of attempting to acquire log-in details by systematically testing their validity via the trial-and-error method. Perpetrators of such attacks usually benefit from the fact that their targets do not often apply multi-factor authentication (MFA) when using online services.

If a device or data is compromised by the means of one of the methods above, the attacker can exfiltrate or attempt to exfiltrate data. Similarly to previous years, the BIS noted interest of attackers in emails or specific types of files (mainly text or image documents) which might be used for maximum extraction of information.



# **Intelligence and Subversive Activities Targeting the Czech Republic**





# Russia



In 2020, Russia and its intelligence services still had the advantage of a disproportionate diplomatic representation. Russia therefore had two key advantages: a more suitable position in case of reciprocal measures against diplomatic personnel and sufficient numbers of qualified personnel present at the time of movement restrictions, which were part of the anti-pandemic measures.

Nevertheless, the anti-COVID measures disrupted the action plans of the Russian diplomacy and intelligence services – travel restrictions necessarily brought about a lack of opportunities for intelligence exchanges in the traditional areas of interest, such as politics, the academic sphere or trade. The Russian interest in contacts with Czech pro-Russian and anti-establishment entities and attempts to use the limited opportunities to build contacts in the regions within the framework of war remembrance events to the maximum all the more increased. Russia aims to use the Czech territory to gain access to Czech nationals but also to build contacts with foreign nationals.

Russia also continued its cyber activities aimed against the Czech Republic.

In the area of Russian influence operations, the priority in the past year remained the promotion of Russian interests presented as also Czech interests, but in fact harmful for Czech interests. Globally, the paradox of Russian influence operations was steadily growing, with narratives directed at Russian audience claiming that Russia is surrounded by enemies, and narratives directed at Czech (or global) audience emphasising that Russia is our saviour.

It initially seemed that the so-called ricin affair bore signs of a subversive attack. The BIS obtained information about an alleged import and planned use of the poisonous substance against Czech politicians. Upon verifying intercepted indications, however, it emerged that it was in fact solely an attempt to involve Czech security forces into an internal dispute between two members of the Russian diplomatic mission. Nevertheless, the BIS inclines towards the possibility that this incident might have been, at least in its final stage, orchestrated by the intelligence services of Russia. As soon as the Czech security forces





informed on some important elements of the enquiry, it became exceptionally difficult to determine whether the threat was real.

There were also continuing efforts of Russian companies linked with the local military-industrial complex to obtain products listed as internationally controlled items from the Czech Republic. The increase in such demands was due mainly to replacement and modernisation of machine tools supplied to Russia in the past. As for military material trade, EU sanctions against Russia, which do not allow for such trade, proved effective.

## China

China also represents a complex growing intelligence threat. At the same time, the question of who is and who is not a Chinese intelligence officer is becoming obsolete – according to Chinese law on national intelligence, every Chinese citizen might be obliged to carry out the will and interests of Chinese intelligence services. Pursuant to applicable legislation, all organisations and

citizens ought to support, assist and participate in national intelligence activities. For Chinese entities and individuals, cooperation with Chinese forces is thus mandatory by law, and refusing to cooperate has serious repercussions.

Despite movement restrictions, Chinese intelligence services were active in the Czech territory also in the past year, mainly under diplomatic and journalistic cover. Chinese intelligence activities were most intensive in the area of politics and scientific and technical intelligence. In terms of possible economic and know-how loss, however, the Chinese intelligence interests and activities posing the most threat are those targeting Czech academic institutions in the form of intensive information as well as influence operations. As for political intelligence, Chinese intelligence services' officials are highly successful in building rapport with individuals active (or influential) in politics, regardless of ideological views.

Influence operations serving Chinese interests focused on shifting the blame for the COVID-19 pandemic on Western countries and on disrupting Czech-Taiwanese political and





economic relations. As part of the influence operations, Chinese intelligence officers, diplomats and members of party organisations were looking for ways to influence public opinion, disseminate Chinese propaganda and build a positive image of China in the Czech Republic by openly or covertly influencing Czech media content. In the context of the COVID-19 pandemic, we can also mention Chinese efforts to buy protective equipment in the Czech Republic.

Within its “Made in China 2025” programme, China continued its efforts to acquire advanced technologies and related know-how from abroad, including from the Czech Republic. At present, China aims to acquire newly developed technologies, such as robotic and autonomous systems, additive 3D print production or nanotechnologies. Chinese entities also undertook further acquisitions of Czech companies of interest and made attempts to transfer production to China or use reverse engineering methods.

## Iran



In the last years, after a few quiet decades, we can again observe an increase in the

activities of Iranian special services in Europe as well as their growing aggression mainly against opposition to the regime in exile. This is why in 2020, the BIS focused on possible security threats linked to the activities of Iranian exile in Europe (possible attacks on opposition journalists or political activists from within Kurdish, Sunnite or generally progressive ideological opposition to the regime). In the Czech Republic, the body which might be affected by such activities of Iran is the Persian redaction of Radio Fardá under Radio Free Europe/Radio Liberty, which Iran perceives to be an opposition entity. Nevertheless, the BIS did not note any indications of an imminent danger in this regard in 2020.

Iran also made efforts to acquire findings which might be used for proliferation from Czech scientific institutes and universities of especially technical focus or at conferences with international participation. Efforts to acquire such findings form part of the so-called intangible transfer of technologies and of providing “technical assistance”, which also involves sharing findings and knowledge in science, research and in business. Proliferation risks linked to the issue of “intangible transfer of technologies” might be mitigated also by continuously raising awareness about their existence.





# Cyberattacks

Although most attack identified and investigated by the BIS over the past year targeted national authorities, the BIS also identified a number of cyberattacks targeting Czech political parties and non-governmental or non-profit organisations. Attacks investigated by the BIS mostly aimed to compromise computer networks or e-mail accounts and to steal data. It was established that the perpetrators of an attack against one of the Czech national authorities accessed a considerable volume of documents.

Attacks against national authorities allow attackers to access information regarding the Czech Republic's aims and policies in specific areas of interest as well as information on individual government employees and representatives including their views on certain topics (e.g. various comments and changes in multiple versions of stolen documents) or their relations with other employees (e.g. leaked correspondence). Stolen data makes all concerned persons vulnerable to traditional methods used in espionage.

disconnection



mass engine 75%

involved computers 1 437

running cloud computers 1 327:34

yield: nullam lacinia pulvinar  
mollis sed, tempus ac  
consectetur risus a  
tristique sed, in d

loading 82%



speeding of loading



speeding of loading





On top of that, private (as well as work-related) e-mail accounts of government employees usually contain a vast amount of personal information such as copies of identification documents, login credentials for various services (e.g. other e-mail accounts, social media, e-shops etc.). In some cases, attackers, such as state and state-sponsored actors, may find this kind of data much more valuable than internal communications of the national authority, which the victims work for. If stolen, the above-mentioned data can be later used to launch a targeted cyberattack against a specific employee or one of the top public representatives and it also increases their vulnerability to traditional espionage methods.

When a national authority's network or an employee's e-mail account is hacked, it can lead to a hack and leak scenario, i.e. stolen information is gradually made public in order to launch a preconceived disinformation campaign, which might aim to defame the targeted national authority, specific public representative/employee or the Czech Republic as a whole. Moreover, a fake piece of information (e.g. made-up documents, photographs or e-mails) can be used in the hack and leak disinformation campaign and published along with authentic documents stolen during the initial attack. The victim of a disinformation (defamation) campaign has virtually no means to protect itself and the campaign has an immense and often irreparable impact on the public's trust in the targeted national authority or individual.

The attribution of cyberattacks must be regarded as a long-term process, which can take months and in some cases, may never achieve the desired results. The

main instruments for attack attribution are technical analysis and all-source intelligence analysis of the attack.

The technical analysis focuses on the tools, methods and infrastructure used by the attack's perpetrators. In general terms, it can be said that attackers have moved to some extent from using their own tools (e.g. malware) to using tools which are freely accessible (e.g. Mimikatz, PowerShell, Cobalt Strike). They also rarely use their own infrastructure, namely servers controlled and managed by the attackers, and they use more and more often hired infrastructure (VPS provided by large companies for a very short period of time, chained commercial VPNs for anonymization purposes and services such as Dropbox, Google Drive etc.). All these elements are great obstacles to positively identifying the perpetrators of an attack.

The all-source intelligence analysis is based mainly on examining open and specialist sources (e.g. reports by research companies), and establishing a correlation between attacks and information acquired thanks to international cooperation, which proves to be an invaluable asset in any cyberattack investigation.

Attribution of cyberattacks is paradoxically made difficult by the extremely well researched specialist reports published by security companies, which describe in detail the attacks by state/state-linked actors. The reports often contain elaborate analysis of the techniques and tools used by the identified attackers and therefore make it easy for other advanced state/state-linked actors to reproduce or emulate the described techniques when launching a false flag attack.





# National Economic Interests

The year 2020 was marked by the preparations of a government tender for the construction of a new nuclear reactor at the Dukovany power plant. Given the great economic significance of the construction project, which will inevitably lead to a decades-long future strategic partnership in the field of energy, one of the main tasks with regard to the protection of major national economic interests was to assess what risk the project could potentially encounter. The most important threat to the project was the potential participation of entities which are the subject of justified concerns that they would use their position to promote their own interests or interests of a third party (mainly geopolitical interests of a foreign state) to the detriment of the Czech Republic.

Before the tender was launched, the main concern was that the preparations and decisions on important issues and conditions related to the tender could be manipulated. In this regard, the BIS identified attempts to acquire information from within the Czech public administration and other entities

involved in preparatory stages of the project. Other activities were also underway, aiming to shape the media landscape and influence key individuals in the decision making process. These activities did not take the form of ordinary lobbying, as it was clear that there were efforts to conceal the origin of information published by the media with the help of seemingly independent persons.

Similar concerns regarding interference with the independent work of the authorities in question and exploitation of documents of seemingly independent nature have long applied to the functioning of national regulatory and supervisory authorities, mainly in the field of energy, telecommunications and health. The conduct of some of the regulated entities in 2020 confirmed the above-mentioned concerns, as activities similar to those in the past were observed. The regulated entities covertly attempted to initiate changes to important legislative norms with potentially far-reaching economic consequences for the Czech Republic. During their involvement in the legislative process, they tried concealing



that they are the actual originators of the proposed legislation by creating an illusion of impartiality.

Apart from the above-described long-term strategies, we have also encountered a new phenomenon, as entities, which are the subject of regulation, became involved with the process of designing regulatory frameworks at its very beginning, gaining important influence over the content of legislative proposals. The involvement of regulated entities in the making of relevant legislation is not undesirable as such, since it can be beneficial at certain stages of the process. However, if the task of creating key documentation is initially given to the regulated entities – e.g. because competent public authorities are short of necessary resources – the regulated entities are given considerable chance to modify the legislation to their own advantage.

The BIS also repeatedly observed efforts by regulated entities to develop irregular links and access to representatives of regulatory authorities or public administration officials. Irregular approach towards some of the regulated entities meant that they were given a number of favours, i.e. when the entities stepped back from opposing certain regulatory measures, they were given advantages in negotiations of other issues.

One of the most important events in the telecommunications field was the auction of 5G cellular network frequency bands. Since previous electronic auctions conducted by the public administration had been subject to occurrences with negative impact on their outcome, it was inevitable to expect that there could be attempts to manipulate the 5G frequency band auction, too. Given past experience, the main risk was that auction participants could follow their own secret agreements. The findings of the BIS confirmed that in the past, some of the entities participating in the 5G frequency band auction in 2020 had historic ties between each other, mainly in terms of their staff and mutual

cooperation. During the course of 2020, no specific covert agreements regarding the frequency band auction were identified.

Public tenders in general have long been jeopardized by possible secret agreements between participants and the year 2020 was no exception. Cartel agreements were made mainly by entities applying for transport infrastructure tenders. Moreover, a new phenomenon, which could potentially have a serious impact on final prices of tenders, was observed as a number of entities providing advisory and support services to public tenderers were in a conflict of interests. New public tenders were generally impacted by the pandemic and the subsequent state of emergency. A need has arisen to procure certain goods in relatively short time (namely medical supplies), which inevitably affected the screening of potential suppliers and allowed entities with no trade history or with non-transparent sources of capital to win tenders.

The sale of a major Czech machinery producer to Russian investors was as good illustration of a case in which national authorities lacked effective tools to prevent investments of potential security concerns or at least to limit the risks created by such investment. Despite the EU's sanctions against Russia, the management of the Czech company publicly announced that it accepted trade deals with Russia shortly after the sale and the company's new owner threatened to move production lines to Russia if the deals were to be stopped. Since a number of machines produced by the company are internationally controlled items, there has been a risk that the transfer of production to Russia could mean that Czech authorities would lose control over the subsequent use of goods, which could be misused for proliferation purposes. During 2020, the new Czech legislation creating a mechanism for investment screening in accordance with EU regulations was finalised, allowing the Czech Republic to improve the protection of the its security.

# Violent and other Activities against Democratic Principles



The COVID-19 pandemic accelerated existing long-term trends in the extremist landscape and showed that it underwent a significant transformation. Even though extremist activities can easily become the subject of sensational news and attract a lot of attention, the real potential of these activities to mobilize new supporters is limited as are the skills of most members of organized extremist groups, which have been experiencing a period of stagnation. Regarding the protection of our country's democratic principles, organised extremist groups in the Czech Republic do not represent a serious security threat since a number of years.

Furthermore, the activities of paramilitary and militia groups have not represented a substantiated threat. Militias strived to look

as professional paramilitary organisations, but in reality, it was nothing more than a fake impression in the media and the groups actually had very small outreach. Militias focused mainly on rallies involving paramilitary drill and similarly oriented lectures. During the course of the year, militias also took part in spreading disinformation and conspiracies regarding COVID-19 and pandemic-related restrictions, using mainly their websites and social media accounts.

However, there are increasingly strong concerns regarding groups and individuals who focus their activism on random issues, while having only negative and often irrational attitudes towards various phenomena instead of a comprehensive system of values or views.



Generally, the main threat is the potential self-radicalisation of individuals who evade the attention of national security authorities thanks to their lack of links to the extremist scene. For the time being, these individuals have focused on moderately serious criminal activities. However, other countries have learnt from experience that this kind of action can lead to violent crimes and even terrorist attacks.

Despite the elevated number of terrorist attacks carried out throughout Europe, the threat of religiously motivated terrorism remains low in the Czech Republic. Even though the BIS detected a few new supporters of radical Islam who were mainly individuals of North African origin and had important ties to the Czech Republic (i.e. Czech residence permit holders, individuals travelling between European countries), they did not constitute a direct security threat according to information available to the BIS. Moreover, no returnees from jihad combat zones were detected by the BIS in the Czech Republic. In 2020, the BIS also continued to monitor the transit and arrivals of individuals with direct links to terrorist groups – however, none of these travels involved a plan to launch a terrorist attack in the Czech Republic.

In 2020, more than ten terrorist attacks were carried out by Islamists on the European soil, making the total number of terrorist attacks several times higher than in the previous year. This was the first yearly increase since 2016. Most of these attacks were not very complex actions and caused relatively few casualties. They were mostly carried out by perpetrators inspired by jihadist propaganda on the Internet. In 2020, some countries became the target of an Islamist terrorist attack for the first time (i.e. Austria and Switzerland). It became clear that the terrorist threat is still present and does not concern only countries with a long history of terrorist attacks.

The main factors, which contributed to the high number of terrorist attacks in 2020, were the increasing number of radicals released from prison and the renewed issue of contentious caricatures of Muhammad. Attacks inspired by

Muhammad caricatures showed that an action targeting the symbols of Islam has greater potential to mobilise radicals than the idea of global jihad. These factors were amplified by other long-term factors such as jihadist propaganda on the Internet or mental health difficulties. In some cases, mental difficulties were the reason why the perpetrators became vulnerable to manipulative propaganda techniques used by Islamist terrorist organisations, e.g. Al-Qaeda or the so-called Islamic state.

Islamic networks, which are a persistent source of jihadist terrorism, continue to exist and take advantage of jihadist propaganda on the Internet. After a seemingly uneventful period, the networks have been reactivated by a number of coinciding factors and events. These include most importantly renewed armed conflicts involving Muslims, growing tensions between Muslim minorities and other parts of societies, consequences of climate and economic changes or other sources of instability. The main elements behind the present growth of Islamic terrorism are the discontent and frustration, which spread among mentally vulnerable individuals who are easy targets of ideological manipulation.

New waves of terrorist attacks are frequently triggered by incidents such as those related to Muhammad caricatures, headscarf ban debates and acts of islamophobia. Jihadist propagandists – who are often radical preachers of hate against people seen as non-believers by Muslims – have shown great skill in using the above-mentioned incidents to recruit new supporters. Even though the international fight against terrorism has been successful in many regards, it is impossible to prevent every single attack perpetrated in the name of Islam. The main reason is that Islamist-jihadist ideology is based on ambivalent ideological sources with great potential to mobilise people. In the future, all countries concerned will therefore be obliged to deal with further attacks of so-called lone actors who became radicalised on the Internet.

لا إله إلا الله

الله  
رسول  
محمد

لا إله إلا الله  
الله أكبر



# Protection of Classified Information, Security and Crisis Management







The year 2020 brought no significant changes to the domain of protection of classified information. Similar to previous years, the BIS drew up expert opinions and assessed the classification of documents in accordance with the Act No. 412/2005 Coll. Within its sphere of powers, the BIS also provided interpretation of the list of classified information and related internal regulations and provided methodical support to the Service's sub-units.

The provision of the information security is regulated by the BIS ICT Security Policy that focuses on continuous improving the security of ICT systems and services provided by application of suitable technologies in both classified as well as unclassified systems.

All classified information systems within the BIS are certified by the National Cyber and Information Security Agency (in Czech: Národní úřad pro kybernetickou bezpečnost – NÚKIB). In 2020, the information system for processing information classified as Confidential and Secret was successfully re-certified.

All users of certified information systems are trained in accordance with the Act No. 412/2005 Coll. before accessing the systems for the first time and then undergo annual trainings, including the raising of awareness regarding the cyber security. In 2020, no serious security incident was detected within the Service.

In the domain of cryptographic protection of classified information, the preparation for

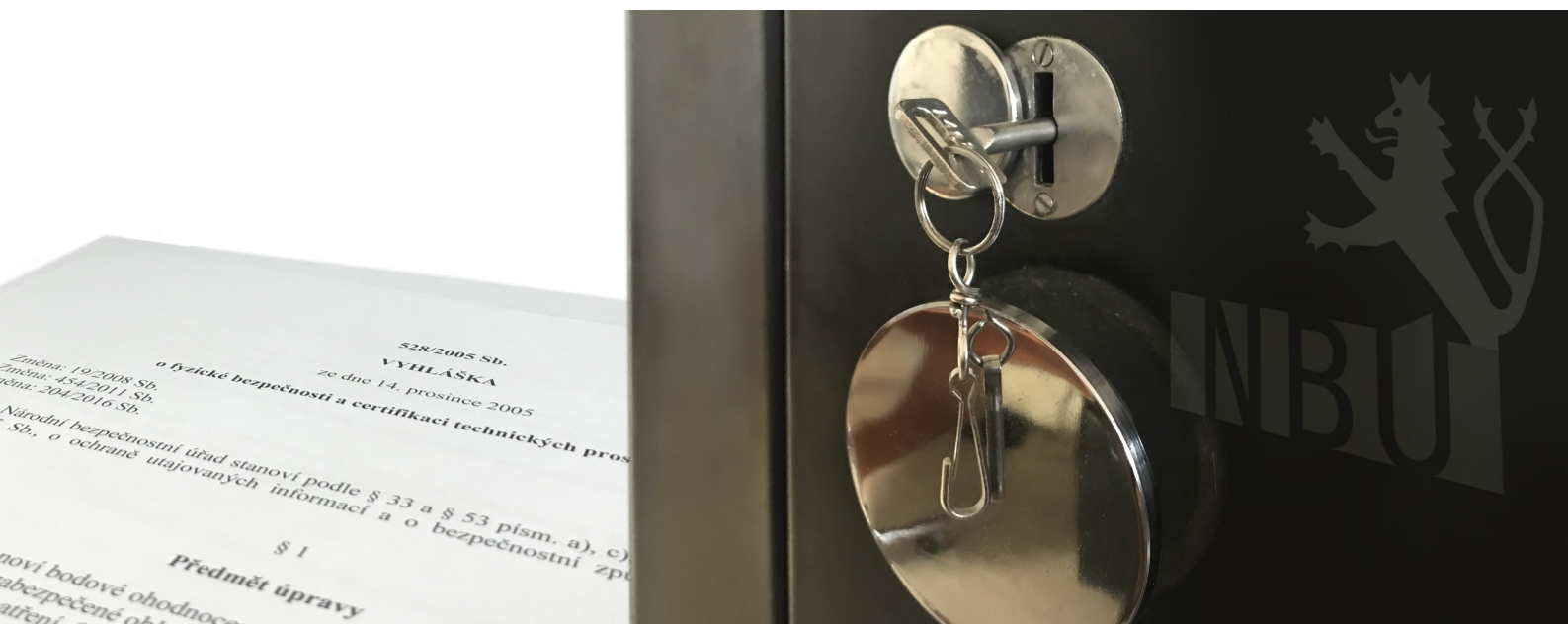
a new system of classified communication with partner intelligence services was made. On the ground of NÚKIB's requirements, a reorganisation of cryptographic protection workplaces of the system took place and a new workplace intended for generation of key materials for this communication system was created. During 2020, security mechanisms were updated in consequence of certifications of both new and current cryptographic devices.

In 2020, the BIS detected no serious incidents or disclosure of cryptographic devices. Cryptographic material was regularly inspected and no shortcomings in management and manipulation have been detected.

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

For the purposes of protection of classified information in emergencies, building and area security plans and emergency plans have been updated. In accordance with the Act No. 240/2000 Coll. on the Crisis Management, the BIS crisis plan and the crisis preparedness plan of the entity of critical infrastructure was regularly updated.

The crisis committee of the BIS Director General was activated and met regularly during the pandemic.



# **Cooperation with Czech Intelligence Services and with other State Authorities**

## **Cooperation with Intelligence Services of the Czech Republic**

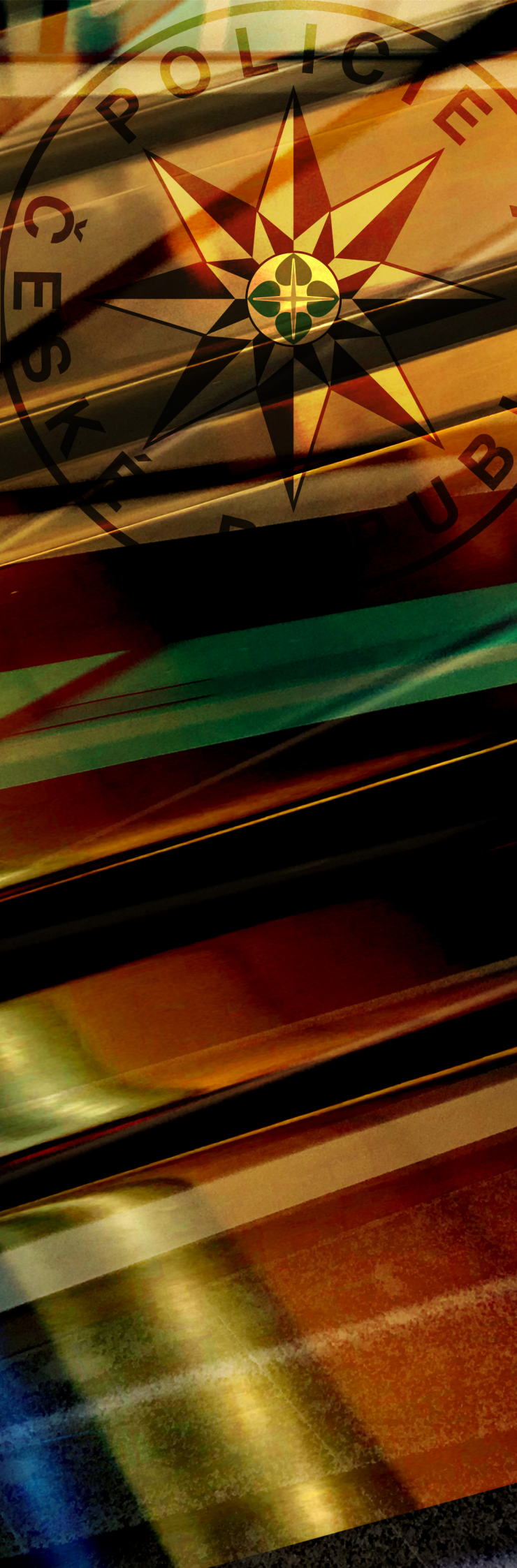
In 2020, the BIS provided dozens of intelligence and findings to the Military Intelligence and the Office for Foreign Relations and Information. Further cooperation with these services takes place at different levels encompassing operational, analytical and technical issues as well.

The BIS cooperated with the Office for Foreign Relations and Information regarding vetting of individuals applying for accreditations as diplomatic representatives and workers of diplomatic missions in order to exclude security risk possibly resulting from the employment of these individuals

in the territory of the Czech Republic. In 2020, the BIS gave opinion on more than one hundred of diplomatic representatives and workers of diplomatic missions.

In 2020, the BIS co-operated with the Ministry of Defence or the Military Intelligence regarding the development of a communication/agenda-oriented information system for the use of intelligence services.

Moreover, the BIS and the Office for Foreign Relations and Information co-operated on training of EU/NATO crisis management bodies or on COVID-19 protective measures.



## Cooperation with the Police of the Czech Republic

The BIS has participated as a guarantor of the common position of the Czech intelligence services in the security risk assessment process regarding visa applications. In 2020, the BIS provided at the request of the Directorate of the Alien and Border Police (in Czech: Ředitelství služby cizinecké policie – ŘSCP) assessment of nearly 400 thousands applications for short-term Schengen visa, which had been submitted at an embassy of the Czech Republic or another Schengen Area country, which then requested cooperation of the Czech authorities. 2020 was influenced by the global COVID-19 pandemic which resulted in significant decrease in the number of the applications. Compared with 2019, the number of the applications was more than four times smaller.

The BIS continued to co-operate with the Directorate of the Alien and Border Police resulting from the Act No. 49/1997 Coll., on Civil Aviation, as amended; which stipulates provisions regarding reliability when accessing security areas of airports. In 2020, the BIS provided assessments of more than 10 000 individual applicants for the reliability certificate which was several thousand applications more than last year. The increase of the number of applications was caused by the necessity to repeatedly assess the reliability of applicants due to the validity of the certificate stipulated to five years by the Act.

The cooperation with the Police National Centre for Combating Organised Crime took the form of exchange of intelligence on major economic interests, terrorism and counterespionage and cyber security. The cooperation concerned e.g. security screening of entities of interest, specifically of members of foreign security bodies striving for specialised training in the Czechs Republic. Findings in the area of economic crime and risks against strategic targets were shared as well.



# Cooperation with other State Authorities and Institutions

The BIS provides chosen state authorities with information and stances regarding security screening of individuals and companies both based on legal regulations and on interdepartmental co-operation. The National Security Authority (in Czech: Národní bezpečnostní úřad – NBÚ), Ministry of the Interior and Ministry of Foreign Affairs belong among the most important addressees of information.

Within the security screening, the BIS replies to the National Security Authority's requests in accordance with Section 107 Paragraph 1, Section 108 Paragraph 1 and Section 109 Paragraph 1 of the Act No. 412/2005 Coll. (i.e. administrative inquiry) or it actively participates in security screenings regarding personnel and industrial security and security clearance background checks in the form of procurement of information in place based on the National Security Authority's requests in accordance with Section 107, Paragraph 2 and 3, Section 108 Paragraph 2, 3 and 4 and Section 109 Paragraph 2 of the Act No. 412/2005 Coll. (i.e. field inquiry). Filed inquiries involve standard intelligence activities including the use of surveillance equipment and techniques for information gathering.

In 2020, the BIS conducted more than 18 000 investigations in registers based on the National Security Authority's requests. After investigations in place, the BIS gave opinions on 107 natural persons and 7 legal persons.

In this domain, besides the National Security Authority's requests; the BIS, within its scope of authority, procures 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. The BIS then provides the National Security Authority with possible


relevant information without delay, if this does not jeopardize an important intelligence interest of the Service.

In 2020, the BIS continued to co-operate with the Ministry of the Interior concerning the assessment of foreigners applying for residence permits or Czech citizenship. The cooperation also concerned vetting of legal and natural persons applying for permits for employment facilitation services.

The Ministry of the Interior and subordinate entities provides the BIS, on the basis of an agreement, with services regarding communication technologies, fire prevention, occupational health and safety, power engineering, water management, environment and also canteen meals. In cooperation with the Ministry of the Interior, the BIS also provided assessments for meetings of the Committee for Civil Emergency Planning. During the COVID-19 pandemic, the BIS cooperated with the General Directorate of Fire Rescue Service (in Czech: Generální ředitelství Hasičského záchranného sboru) regarding protective devices, counter-epidemic measures etc.

The BIS also cooperated with the Security Policy Department of the Ministry of the Interior on vetting of legal and natural persons applying for permits for employment facilitation services according to the Act No. 435/2004 Coll., on employment. The BIS vetted more than 1300 natural and almost 700 legal persons.

The cooperation of the BIS and the Department for Asylum and Migration Policy of the Ministry of the Interior consists in elimination of security risks regarding foreigners applying for residence permits granted according to the Act No. 326/1999 Coll., on the residence of foreigners in the Czech Republic and amending certain Acts;



and foreigners applying for international protection according to the Act No. 325/1999 Coll., on asylum.

In 2020, the BIS provided assessments of more than 124 000 applicants for residence permits. Compared to 2019, it assessed 15 000 less applications, which has been the first decrease in the number of applicants since 2016. The decrease was probably caused by the global COVID-19 pandemic and related measures.

In 2020, the BIS also cooperated with the Department for Asylum and Migration Policy on vetting of individuals within Medical Humanitarian Programme MEDEVAC. In 2020, the programme was focused on providing help for Belarusian citizens. The BIS vetted 90 individuals of Belarusian and Russian citizenship who were transferred to the Czech Republic in connection with the conflict in Belarus.

In 2020, the BIS provided at the request of the General Administration Department of the Ministry of the Interior assessment of more than 3500 applicants for Czech citizenship according to the Act No. 186/2013 Coll., on citizenship of the Czech Republic.

The BIS continued to cooperate with the eGovernment Department of the Ministry of the Interior on vetting of applicants for the accreditation to manage qualified electronic identification system according to the Act No. 205/2017 Coll. on electronic identification.

Furthermore, the BIS has cooperated with the Security Department of the Ministry of Foreign Affairs. The cooperation consists mainly in elimination of security risks regarding both natural and legal persons cooperating with the Ministry or applying for the cooperation with the Ministry. In 2020, the BIS assessed security risks of more than 500 natural and 30 legal persons.

The BIS regularly shared intelligence information within the Joint Intelligence Group (in Czech: Společná zpravodajská skupina) and the National Contact Point for Terrorism (in Czech: Národní kontaktní bod pro terorismus – NKBT). Within the Joint Intelligence Group, the BIS contributed to evaluation of security



situation regarding possible danger to the Czech Republic. The influence of quarantine measures on terrorist attack threat evaluation, impact of current terrorist attacks and situation in foreign mission of the Czech Army in Mali and Afghanistan were the main topics. The cooperation within the NKBT consisted mainly in vetting of identities gathered in connection with investigation of terrorist attacks in the EU.

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

In 2020, the BIS also cooperated intensively with the General Inspection of Security Forces (in Czech: Generální inspekce bezpečnostních sborů – GIBS), Financial Analytical Office, Customs Administration (in Czech: Celní správa ČR), Prison Service (in Czech: Vězeňská služba ČR), General Financial Directorate (in Czech: Generální finanční ředitelství), courts and public prosecutors.

Cooperation with other national administration bodies also pertained to specific cases of proliferation of WMDs and their carriers and trade in military material. Cooperation was conducted primarily with customs administration bodies both on the level of the General Directorate of Customs and individuals customs directorates. The BIS continued its cooperation with customs administration bodies in order to prevent potential export of controlled items, i.e. primarily military material and dual-use items, to sanctioned countries. In specific cases, the Service cooperated with the Ministry of the Interior, Ministry of Defence, Ministry of Foreign Affairs, Licensing Administration of the Ministry of Industry and Trade, State

Office for Nuclear Safety (in Czech: Státní úřad pro jadernou bezpečnost – SÚJB) and their subordinate organizations, with aim to contribute to authorization and licensing proceedings and to provide information on the compliance with license conditions and requirements of international control regimes.

The BIS cooperated with other state authorities on securing information on activities, the consequences of which may jeopardize the security or major economic interests of the Czech Republic. The BIS communicated with the General Financial Directorate concerning its authorisation to gain information from tax proceedings. The BIS also shared information with prosecuting authorities, the State Office for Nuclear Safety and the Office for the Protection of the Competition belonging to the scope of their action. Moreover, the BIS consulted with executive authorities, mainly with the Ministry of Industry and Trade and Ministry of Interior, regarding preparations for the construction of a new nuclear source and with the Ministry of Industry and Trade regarding vetting of foreign investments.

Active cooperation also continued within the Interagency Body for the Fight against Illegal Employment of Foreigners. The Body deals e.g. with inspecting activities concerning economic activities and stay of foreigners in the Czech Republic, legislative and non-legislative materials regarding stay and employment of foreigners, activities of employment agencies and last but not least activities called as undeclared work.

The cooperation with the National Cyber and Information Security Agency concerned not only the protection of classified information within physical security but also sharing of intelligence information.

In 2020, the BIS also cooperated with state authorities within the fight against the COVID-19 pandemic. The cooperation with the Ministry of Industry and Trade and State Material Reserves Administration consisted namely in provision of protective devices and disinfections.

# Cooperation with Intelligence Services of Foreign Powers

Cooperation with intelligence services of foreign powers is provided for in Section 10 of the Act No. 153/1994 Coll., on intelligence services of the Czech Republic. The BIS is authorized to cooperate with over a hundred of intelligence services. The BIS exchanges information and stays in active touch mainly with the services from EU and NATO member countries and some other countries. As far as multilateral cooperation is concerned, the BIS was active in several organizations, e.g. the Counter-Terrorism Group or NATO Civilian Intelligence Committee.

Considering limited possibilities of travelling abroad and organising of international meetings, interactions with partner services took place mainly via

electronic communication means. It seems reasonable to expect that these means will be used and developed also in 2021.

The BIS received more than 10 000 reports from its foreign partners and sent ca. 1800 documents. BIS representatives took part in more than 500 international strategic and expert meetings.

The total number of received and sent reports was a little lower than last year, which can be ascribed mainly to the necessity to prioritize the international cooperation due to limiting anti-pandemic measures on the part of the services.

The cooperation focused mostly on the fight against terrorism, counterintelligence, proliferation, cyber security, protection of classified information and security eligibility.



# Oversight



The 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.

However, the Act No. 153/1994 Coll. defines neither the scope nor the manner of Government oversight. The Government's oversight powers are based on its entitlement to assign tasks to the BIS and to assess their fulfilment. The BIS is accountable to the Government, which also coordinates its activities and appoints or dismisses the Director General of the BIS. The BIS must submit reports on its activities to the President and to the Government once a year and whenever it is requested to do so. This shows that Government oversight focuses on all activities of the Service.

The Chamber of Deputies, i.e. its respective body for intelligence services, is informed about the activities of Czech intelligence services by the Government. This special oversight body is the Standing Oversight

Commission. Authorized members of the oversight body may, e.g., enter the Service's buildings when accompanied by the BIS Director or by a BIS official designated by the Director for this purpose; or request due explanation from the BIS Director should they feel that the activities of the BIS illegally violate the rights and freedoms of the Czech citizens. The Director General of the BIS is obliged to provide legally defined information and documents to the Oversight Commission.

The Act No. 325/2017 Coll., amending the Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic, as amended, and other relevant acts assumes the establishment of a five-member expert oversight body, the Independent Authority for the Oversight of Intelligence Services of the Czech Republic. 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. 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 with several exceptions. This Authority has not been established yet.

Oversight regarding the Service's management of state-assets and of the funds allocated to the BIS from the state budget is stipulated in the Act No. 320/2001 Coll., on Financial Audit in Public Administration and on the Amendments to some Acts, as amended, and in Regulation No. 416/2004 Coll., implementing this Act, and in the Act No. 166/1993 Coll., on the Supreme Audit Office, as amended.

The protection of the classification of the operation of intelligence services requires special execution of oversight activities. 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. If the intelligence service is not able to arrange for such oversight activities within the scope of its powers and responsibilities, it is obliged to allow for their execution by the oversight body. The service may require special conditions related to the oversight proceedings.

The Service's operations are also subject to judicial oversight of the use of intelligence technology in accordance with the Act No. 154/1994 Coll. 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. The Chairman of the Panel of Judges of the High Court in Prague also rules on the Service's requests for reports from banks on matters related to their clients and subject to bank secret. The Court not only issues warrants based on a written request submitted by the BIS, but also supervises, whether the reasons for the request remain. If not, the Court cancels the warrant.

The public usually conducts oversight via mass media or the BIS website, where annual reports or other announcements regarding security situation are available.

## Internal Oversight and Internal Audit

Expert units of the BIS conducted 11 inspections. Their aim was to methodically and factually guide the operation of organisational units in the financial and material area and prevent potential emergence of undesired phenomena. Individual inspections were focused e.g. on accounting and budget, material and technical provision and property records, reimbursements of travel expenses, benefits from cultural and social needs funds, monitoring of technical condition of vehicle and MOT testing, observance of control norms for fuel consumption and observance of vehicles employment. No severe infringement of regulations was uncovered within these inspections.

The BIS Sickness Insurance Body carried out three inspections of persons temporarily unable to work. No infringements of regulations were uncovered.

Employees of the archive and of the control group carried out 20 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.

The BIS internal audit service operates in compliance with the Act No. 320/2001 Coll., on Financial Control in Public Administration and on the Amendments to some Acts, as amended. In 2020, three audits were completed. No severe infringement that could adversely influence activities of the Service or signalise reduced quality of its internal oversight system were identified.



# Maintenance of Discipline; Handling Requests and Complaints

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 Letter f) of the Code of Criminal Procedure, on suspicion of commitment of a criminal act by a BIS official; investigation of conduct suspected of having the traits of a misdemeanour and of a disciplinary infraction by a BIS official, including emergencies; investigation of complaints, notifications and motions by the BIS officials and external entities; processing requests submitted by other law-enforcement authorities in accordance with the Code of Criminal Procedure and requests by other state administration authorities.

The majority of investigations of conduct suspected of having the traits of misdemeanour or disciplinary infraction related to transport, e.g. traffic offences with service or private cars, damage to service cars and suspicions of other violations of the act

on road traffic. Cases of conduct suspected of disciplinary infraction or of having traits of a misdemeanour by a BIS official were referred to a disciplinary proceeding.

None of 250 reports was evaluated as a complaint about conduct of a BIS official. All reports were examined and evaluated and no violations of internal or generally binding legal regulations on the part of a BIS official were found; and further procedures were set. In terms of content, reports made by citizens reflect society-wide developments in the Czech Republic and abroad, and situation concerning the COVID-19 pandemic.

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





# Budget

The budget of the BIS was stipulated by the Act No. 355/2019 Coll., on the State Budget of the Czech Republic for 2020. Approved revenues amounted 190 000 thousands CZK and expenditures 2 147 315 thousands CZK. Besides, the BIS registered claims to unconsumed expenditures as its only source outside budget. Total real revenues amounted 254 573 thousands CZK. Total real expenditures, including employment of claims to unconsumed expenditures, amounted 2 208 004 thousands CZK as of 31 December 2020.

Service's funds were invested besides construction of a technical and administrative compound also in maintaining of serviceability of material and technical base and its most necessary development within purchase and technical renovation of BIS property including common periodic renewal. Another necessary investment has been allocated to information and communication technologies and intelligence technologies. The aim was to provide the necessary server capacity and adequate communication technology solutions as well as advanced software tools, which would allow better processing, storage and analysis of intelligence information. Further expenditures were made in order to improve the security of intelligence work and data. A significant amount of funds has been used for the continual renewal of the Service's vehicle fleet.

Payroll expenses traditionally accounted for the majority of common expenditures,

including salaries and equipment payments and severance benefits, i.e. mandatory payments to retired personnel.

Further regular expenditures were comprised mainly of spending on special equipment necessary for the operation of an intelligence service. Other operational expenditures, e.g. common material expenditures, expenditures for purchase of services and energies and outsourced services and maintenances of property and compounds of the Service did not deviated from the trend of last years. Unplanned expenditures related mainly to hygienic and organisational COVID-19 measures to provide safe and healthful regime in workplaces. In 2020, the Service's readiness for action was not fundamentally violated also thanks to timely taken measures.

In 2020, the funds allocated to the BIS allowed all basic operational and development requirements to be fully covered. Just as in the past years, it was necessary to employ claims to unconsumed expenditures in funding of developments of intelligence technologies, information and communication technologies and the construction of the technical and administrative compound. On the contrary, it was not possible to use common expenditures planned e.g. for training courses, conferences, and foreign business trips because of valid epidemiological measures. Furthermore, several smaller investment projects were cancelled or postponed on the part of the BIS or suppliers.



## **Annual Report of the Security Information Service for 2020**

### **Contacts**

Address:

Bezpečnostní informační služba  
P. O. BOX 1  
150 07 Prague 57  
Czech Republic

Contact for the public:

Phone: +420 235 521 400  
Fax: +420 235 521 715  
E-mail: [info@bis.cz](mailto:info@bis.cz)  
Data box: cx2aize

Contact for media:

E-mail: [press@bis.cz](mailto:press@bis.cz)  
Phone: +420 257 142 007

Contact for prevention:

E-mail: [prevence@bis.cz](mailto:prevence@bis.cz)



