

SECURITY INFORMATION SERVICE

ANNUAL REPORT 2021



**Annual Report of the
Security Information Service
for 2021**

Summary	
A Message from the Director General of the Security Information Service	5
Nature and Scope of Intelligence Activities	6
Intelligence Activities and Findings	8
Intelligence and Subversive Activities Targeting the Czech Republic	
Russia	10
China	11
Iran	12
Cybersecurity	13
Activities contrary to the principles of democracy	15
Major economic interests	17
Violent action, extremism and radicalisation	18
Protection of Classified Information, Security and Crisis Management	21
Cooperation with Czech Intelligence Services and other State Authorities	
Cooperation with Intelligence Services of the Czech Republic	22
Cooperation with the Police of the Czech Republic	22
Cooperation with other State Authorities and Institutions	23
Cooperation with Intelligence Services of Foreign Powers	27
Oversight	28
Internal Oversight and Internal Audit	29
Maintenance of Discipline; Handling Requests and Complaints	30
Budget	31



Dear readers,

I present you with the unclassified annual report on the activities of the Security Information Service, this time for 2021. The following pages will provide a general overview of the issues that our Service focused on in the past year, which I dare say was a crucial year in many ways. It brought many important events which affected the security of the Czech Republic and of its people for years to come.

Most importantly, after several years of intensive police investigation in close cooperation with the BIS, it was made public that the Russian military intelligence service, the GRU, was responsible for the Vrbětice ammunition depots explosions in 2014. The release of this important information provoked a number of measures which fundamentally influenced our relations with the Russian Federation. It also led to a significant change in the existing perception of Russia and in particular of the security risks associated with this country.

The operation of a foreign intelligence service in the territory of a sovereign country, which caused the death of two innocent people and billions worth of damage on state and private property, was a tragic confirmation of risks which the Security Information Service had warned against for many years. Our warnings that the Russian Federation presents a serious security threat to the Czech Republic as well as Europe materialised with even more serious consequences in 2022 in the form of the Russian aggression in Ukraine.

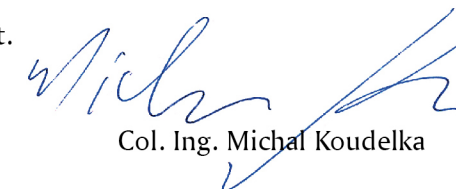
In 2021 in a very short space of time, the Government and the vast majority of the national political representation agreed to apply unprecedented measures; after many years of the Russian Embassy in the Czech Republic being overstaffed and for the first time since the establishment of the Czech Republic, our country reached parity in this area with the Russian Federation. Furthermore, Russia was excluded from the Dukovany nuclear power plant completion works tender.

Despite all these events, the BIS also worked on other tasks determined by its legally defined scope of powers. In 2021, by far the most reports delivered to the entitled addressees by our Service concerned major national economic interests. Apart from that, we focused on the activities of foreign intelligence services, mainly from the Russian Federation and the People's Republic of China. We also devoted our attention to terrorism and organized crime.

We are publishing our annual report in a year when the security situation in Europe and elsewhere changed very radically due to the Russian invasion of Ukraine. The near future will be a test for us all. We are already experiencing the consequences of the Russian aggression, and we will continue to see their impact on our economic and security situation for many years to come. I am certain that the Czech Republic will stand this historic test.

I hope that despite the inevitably general nature of our annual report, you will find it of interest.

I wish you good health, courage and all the best.


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

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

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

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

Intelligence Activities and Findings

From the point of view of security, the principal event of last year was the publication of the results of an inquiry into the explosions of the Vrbětice ammunition depots, which put our relations with Russia into a new context. This was also symbolised by a mass expulsion of Russian intelligence officers operating in the Czech Republic as part of the Russian diplomatic mission. The inquiry into the Vrbětice case still lies fully within the authority of law enforcement agencies, to whom the BIS provides all possible assistance in the matter.

Given that Czech-Russian diplomatic parity has been successfully established, in the following period, we expect bigger Russian influence on the Czech Republic from embassies and consulates abroad.

In terms of Chinese interests, the main trends have not changed significantly. The intelligence work was traditionally oriented towards eliminating the so-called five poisons – activities which the Chinese Communist Party perceives as a threat to the regime. These activities include supporting the independence of Taiwan, Tibet and Xinjiang, Chinese pro-democracy movements and the Falun Gong movement. Apart from that, the Chinese regime took substantial interest in Czech political intelligence. In this context, the BIS identified indications of a growing importance of the Chinese expatriate community in the Czech Republic for Chinese intelligence activities and a Chinese willingness to invest in legitimate academic publishing work, which however eventually

has the potential of transforming into wilful or involuntary cooperation with Chinese intelligence services.

In 2021, the Czech Republic was targeted by several cyber espionage attacks, the perpetrators of which were most likely state/state-sponsored actors linked to Russia and China. The targets of these attacks were both state and non-governmental entities. The Czech Republic was a place where not only the targets were located but also part of the perpetrators' infrastructure used for cyber espionage attacks against other countries.

In the past year, the BIS focused on the detection of possible illegitimate interference or disruptions of the election process by threat actors. The spontaneous disinformation and conspiracy activities of Czech disinformation agents or alternative media that we noted in connection with the elections were marginal. Similarly to 2020, the activities of the COVID-denial movement took place mainly online. The disinformation content spread by the COVID-denial spectrum in general reflected the situation within the society and the evolution of the pandemic in the Czech Republic and worldwide. The BIS did not register any direct influence of a foreign power when it came to organising anti-COVID events or spreading disinformation about COVID-19.

The most serious negative phenomena detected by the BIS in 2021 in terms of protecting major economic interests were attempts to influence the decision-making and legislative processes and manipulate public procurements. In the area of energy security, the BIS looked into the preparations of a new nuclear source construction project in Dukovany, espe-

cially into efforts to influence the project to the benefit of one of the interested parties.

The level of the Islamist terrorism threat in the Czech Republic remained low in 2021. The BIS maintained its primary focus on detecting individuals which might pose threat in terms of conducting a terrorist attack or providing logistical support. The threat of Islamist terrorism in the Czech Republic continued to be influenced by external factors, mainly the security situation in Europe.

In 2021, the activities of far-right extremists were practically limited to sharing opinions online or alternatively to supporting public events and protests organised by other civil-society players. The pandemic also further intensified the stagnation of far-left extremist groups, as they lacked relevant topics and were unable to organise bigger events which they could use to attract suitable audience and to expand their currently very limited ranks of supporters. As for the militias, they were a non-homogenous cluster of several disparate and very loosely interconnected groups in 2021.

Intelligence and Subversive Activities Targeting the Czech Republic

Russia

On 17 April 2021, Czech government representatives informed the public about the involvement of officers of a special subversive unit of the Russian military intelligence service, the GRU, identified as Unit 29155, in the preparations of the Vrbětice ammunition depots explosions, which took place on 16 October 2014 and 3 December 2014. The publication of the results of the inquiry into the explosions of the Vrbětice ammunition depots undoubtedly placed the relations between the Czech Republic and the Russian Federation into a new context, symbolised by a mass expulsion of 18 Russian intelligence officers operating in the Czech Republic under diplomatic cover as part of the Russian diplomatic mission.

Given the asymmetric reaction of the Russian Federation and a further escalation of the situation, May 2021 saw the establishment of diplomatic representation parity of both countries, i.e. even number of staff at both embassies. This led to a forced departure of dozens of workers of the Embassy of the Russian Federation in the Czech Republic – in many cases individuals with links to Russian intelligence services.

It was the first time that the previously disproportionate diplomatic representation, which Russia long used to secure cover for officers of its intelligence services, gave way to a balanced state of affairs. The Russian intelligence services are now forced to look for other options for their intelligence operations in the Czech territory. Given that members of the Russian intelligence services regularly abuse of the free movement of people within the Schengen, the BIS expects an

increase in Russian intelligence operations conducted from abroad, especially countries where Russia maintains a robust diplomatic and intelligence presence.

As a consequence of measures adopted in the aftermath of the Vrbětice affair, members of the Russian diplomatic mission had significantly less opportunities to meet the representatives of Czech pro-Russian activists in person. Nevertheless, one influence agent acting in favour of the Russian state apparatus with links to journalists and indirect links to some politicians was successful in maintaining and extending contacts with pro-Russian activists. This person used these connections to establish a pro-Russian political agenda, coordinate public appearances of implicated politicians and give publicity to narratives in line with the foreign policies of the Russian Federation.

The influence group to which this agent belongs had enough money to maintain or even extend its pool of pro-Russian journalists and activists, who created alternative media content as well as organised public events which the Russian propaganda could use to its own benefit. The individuals involved had their expenses for the preparation of materials covered, and some of them had their trips abroad paid for, their activities there being coordinated and controlled further.

Similarly, some Czech pro-Russian activists were contacted by Russian state media representatives to provide biased comments to be used especially by the Russian domestic propaganda. Through associated activists and journalists and the alternative media scene, which draws significantly from pro-Kremlin narratives, opinions favourable to the foreign policies of Vladimir Putin's regime spread in the Czech Republic.

The year 2021 also saw a further increase in the Russian military-industrial complex demands, especially in the field of machine

tools, materials and know-how as well as military material by the means of re-exportation and ignoring/circumventing international sanctions. In general, it can be said that the EU sanctions currently in place against Russia are effective and force Russian entities to look for alternative ways of getting the goods.

China

Despite the fact that the attention of the Czech society is currently primarily focused on relations with Russia, China poses a growing and complex intelligence threat. In the Czech Republic, Chinese intelligence activities are still at a high level, and in 2021, the BIS detected influence operations involving all types of activities and platforms and promoting Chinese foreign policies to the detriment of Czech national interests.

China continued to exert influence in line with current Chinese foreign policies, especially in connection with deteriorating relations with Taiwan. In this context, Chinese media for instance published highly critical content accusing the Czech Republic of allegedly repeatedly violating the One China policy. China also demanded an immediate end of cooperation between the Czech Republic and Taiwan as a condition for providing the Chinese vaccine against COVID-19.

Aside from influence operations, Chinese intelligence structures used traditional diplomatic or journalistic cover to conduct intelligence activities in the Czech Republic also in 2021. Not only Chinese intelligence officers but also Chinese career diplomats were involved in such activities.

Due to the Czech parliamentary elections taking place, the attention of China focused on political intelligence. China was highly interested in political development predictions, post-election scenarios and possible impact on Czech-Chinese relations. This is why

it sought the services of Czech experts and agencies able to provide relevant analyses and surveys. After the election results brought about the loss of some long-established contacts, China focused on “damage control”, including finding new partners on the Czech political scene.

In its endeavour to navigate the post-election environment and find a new strategy, China was among others assisted by some academics, whose expertise was sought after by not only Chinese intelligence officers but also some Chinese diplomats. Their interest focused mainly on internal EU developments and the consequences affecting the foreign policies of the PRC. For China, exploitation of long-term contacts from academia presents a valuable source of political intelligence, and for the Czech Republic, it presents the threat of top Czech academia being used to the benefit of a foreign power.

Chinese intelligence activities also include using the Chinese expatriate community, which is not very large in the Czech Republic, but it is prone to potential mobilisation by the Chinese state apparatus. On top of the fact that all Chinese citizens and organisations are legally bound to assist with intelligence activities, China also uses state propaganda to ensure unconditional obedience and respect towards the ruling Communist party. By a combination of forced obedience and fear of repercussions for activities aimed against the regime, China creates a network of loyal Chinese expatriates who could be used for Chinese influence operations. The BIS noted an intensive long-standing Chinese interest in using expatriates for influence operations and intelligence work also in the past year.

In the past few years, China has also become one of the most active actors in the field of cyberattacks. There has been an increase in their numbers, but more importantly also in their severity and sophistication. Chinese cyberespionage activities are typically very

technically advanced, long-term, and what is more, they are covert and hard to uncover. They can therefore affect the functioning of targeted institutions even several years following their detection. Chinese technologies penetrating important networks of state infrastructures across the globe or the rise of Chinese technologies of the Internet of things in combination with mass surveillance of the Internet can be evaluated as a major security threat.

While EU and NATO member states try not to provide China with EDT (Emerging Disruptive Technologies), such as artificial intelligence, autonomous systems, hypersonic systems, biotechnologies, nanotechnologies, additive technologies (manufacturing methods using 3D printers and layering) or blockchain, China is working on carrying out its Made in China 2025 programme, including obtaining advanced technologies from the Czech Republic. In this context, the most high-risk activities are China obtaining shares in Czech companies and its attempts to transfer production to China (also by using reverse engineering).

Iran

Iran's intelligence activities pose a long-term security threat to European countries, including the Czech Republic. Iranian intelligence officers are active in various positions in Iran's state as well as private sector. They focus mainly on Iranian opposition entities, on identifying targets of potential attacks and on circumventing current sanction regimes. Iranian intelligence activities can be detected also in the Czech territory, but to date, they have not been very significant.

In 2021, the BIS continued to monitor individuals within the Lebanese community who might maintain ties to the Hezbollah terrorist group, which uses European states mainly as a source of income. The activities of the Lebanese community were significantly limited by the measures against COVID-19 and did not pose a threat to the interests of the Czech Republic.

Cybersecurity

The BIS traced mainly the activities of Russian and Chinese state / state-sponsored cyberespionage actors in 2021, as they attacked targets not only in the Czech Republic but also in other EU and NATO member-countries.

For example, the BIS discovered several elements of infrastructure used by foreign cyber-espionage groups for spreading surveillance malware, exfiltrating data from compromised victims or controlling some of the attackers' in-

The Czech Republic is not only a country where attackers hide their infrastructure but also a regular target of their strikes. There have been strikes against key public administration bodies such as government ministries, the military and various national institutions. On top of that, cyberespionage actors attacked non-governmental, non-profit and research organisations in the field of international relations, human rights, security issues and other economic or political issues linked to activities such as the promotion of democracy.



frastructure in other countries. In one specific case, the BIS was able to gain access to and analyse a whole toolkit used by a cyberespionage actor.

The exposed infrastructure included devices used for a spear-phishing attack against dozens of diplomatic missions of European countries around the world. The attackers exploited a legitimate but long unused email account, which they had gained access to. The BIS has noticed spear-phishing attacks to be conducted by state / state-sponsored actors with the help of legitimate email accounts of real people on several occasions. Usually, the accounts were several years old and mostly unused by their owners.

Apart from attacks exploiting the human element (phishing and spear-phishing), the methods most often employed by advanced actors and cybercrime groups include the exploitation of newly discovered vulnerabilities, i.e. zero-day attacks. Involving both software and hardware products, these vulnerabilities are not known to manufacturers or the cybersecurity community and no security patch is therefore available. Vulnerabilities in popular and widely used products have global impact in terms of cybersecurity on both the state and private sectors. Consequently, the Czech Republic faces the same cybersecurity threats as other nations.

In 2021, attacks with global consequences included those against the Microsoft Exchange

platform / email server, exploiting a series of three zero-day vulnerabilities. As result, the attackers were able to gain administrator access to the server as well as to overtake control completely (which allowed them to access email messages and accounts and in some cases, to compromise the victim's inner network). As soon as security patches for a set of vulnerabilities collectively known as Proxy-Logon became available in early March 2021, un-patched email servers around the world were hit by a wave of strikes.

The attacks were committed by a range of cyber actors (involved in either espionage or crime, including ransomware attacks and crypto mining). As soon as January 2021, the same vulnerability was exploited by several advanced state / state-sponsored actors (commonly referred to as Advanced Persistent Threat – APT), as was successively reported by a number of private cybersecurity companies. Some attackers had links to the Chinese state and certain Chinese groups had been exploiting the vulnerability since as early as November 2020.

Even though security patches were applied reasonably quickly all around the world, some servers were compromised. Following a warning and recommendations by the National Cyber and Information Security Agency (in Czech: Národní úřad pro kybernetickou bezpečnost – NÚKIB), most Czech network operators took action without delay, including entities not regulated by law. In a few cases, email servers fell victims to attackers, including servers both regulated and unregulated by law.

The Log4j Java-based open source logging utility was also affected by a major critical vulnerability which was discovered in December 2021 and which could be found in most open source projects. The vulnerability was exploited by cyber actors of all kinds – including state-sponsored APTs – for attacks on a range of targets. Yet, the BIS did not find this particular vulnerability to be exploited in the Czech cyber environment.



Activities contrary to the principles of democracy

In the course of 2021, the BIS responded to threats emanating from actors whose skillset would allow them to interfere with or disrupt the election process. Among other things, the BIS focused on disinformation campaigns, cyberattacks and potential influence activities by foreign powers.

Disinformation regarding the election process was spread more often by known entities acting as disinformation content multipliers than by externally coordinated campaigns. It has been confirmed that the disinformation scene in the Czech Republic makes pragmatic use of any

new topics which arouse strong emotional reaction. Although there was some disinformation aiming to undermine the public's trust in the election process, the BIS found no evidence of it being spread in a coordinated way. The impact of such disinformation was insignificant.

With regard to the parliamentary election in October 2021, domestic disinformers reused various rumours, lies and manipulative arguments, which were shared mainly among authentic communities. Conversely, coordinated efforts to spread disinformation were mostly driven to the background. The most prominent element in the disinformation ecosystem were websites which either contained disinformation or manipulated true information. Due to their far-reaching

ching popularity, these websites had an impact on the rest of the alternative media scene and their articles were widely shared on social media. Some election candidates or parties were heavily targeted by disinformation due to antipathies held with regard to them by members of the disinformation scene.

In terms of influence activities, the parliamentary election also became the subject of interest to seemingly independent civil organisations which are influence platforms fully under the control of the Russian government.

The disinformation scene in 2021 had an interconnected but decentralized structure and disinformation and conspiracies were spreading mainly within the disinformation scene itself. Disinformers directed their activities mainly towards persons experiencing difficult life situations and discontented or frustrated individuals. A key element of their motivation was to make financial profit, e.g. in the form of financial donations from their audience. Some of them actually happened to make financial gains from disinformation. The organisational structure, financial background and staff resources of disinformation platforms were to a large extent non-transparent. There was often an apparent effort to hide the identity of their owners, editors and contributors. Moreover, the disinformation ecosystem is interconnected. Disinformation continues to spread primarily on Facebook, disinformation websites and through chain e-mails. A part of the anti-establishment scene used Telegram for communicating radical-toned views. The dominant vehicle of disinformation were alternative websites whose content projected into disinformation groups on social media.

Disinformation platforms often displayed narratives consistent with interests of foreign powers (namely the Russian Federation and the PRC). However, numerous disinformers worked on their own initiative and their activity was only loosely inspired by these narratives. Some representatives of anti-establishment and populist political entities took part in spreading the narratives on disinformation platforms.

In the course of the COVID-19 pandemic, disinformation narratives gained increased popularity in the Czech society, as disinformation spread with growing speed on social media. In 2021, the most prevalent narratives in the online disinformation space focused on COVID-19, vaccination and pandemic-related restrictions. Some election candidates were also involved in spreading disinformation during election campaign, increasing the reach of disinformation among the general public.

One of the main sources of the information shared among supporters of the COVID-denial movement were articles published by disinformation media. The BIS noted some disinformation narratives originating from foreign-language websites, too. In the course of 2019, some COVID-denial activists underwent a slow radicalisation in terms of opinion and rhetoric, however, their beliefs and protest activities failed to appeal to the most of the society. Having a mostly symbiotic relation with the COVID-denial movement, pro-Russian activists used COVID-19 as a vehicle for spreading conspiracy theories, disinformation and pro-Kremlin propaganda.

Prior to the parliamentary election in October 2021, some representatives of the COVID-denial movement tried to exploit the reputation which they made for themselves thanks to their COVID-denial activities and ran for election. When the election bids of these entities failed, the COVID-denial scene regrouped, became more interconnected and started to coordinate its activities with more care. At the end of the year, the most prominent activists organised a series of protest meetings, which were attended also by individuals from the anti-establishment milieu (including extremist and militia groups). As a result, the COVID-denial movement facilitated the spreading of radical and extremist views in the society. Similar cooperation within the anti-establishment milieu was unprecedented in the Czech Republic, although the movement's potential for mobilisation remained small and it had almost no society-wide impact.

Major economic interests

Very much like in the previous year, the BIS continued to monitor preparations for the construction of a new nuclear reactor at the Dukovany power plant. Given the significance of the project for the Czech Republic's energy policy, there was an important threat to the project in the form of potential participation of entities which are the subject of justified concerns that they would exploit their position to promote their own interests or the interests of a foreign government.

In early 2021, there were enduring efforts to influence media and public opinion in a way that would be advantageous to a participant in the construction tender. In the meanwhile, representatives of one of the participants exploited their contacts among members of professional and special interest groups within the Czech industrial sector in order to gather information or coordinate future action. As the list of potential candidates was narrowed down, these activities decreased and the threat of entities of security concern taking part in the tender was significantly reduced. Nevertheless, the same threat could resurface again in the future in connection to supply chains which is

why the BIS focused on changes in the ownership of potential sub-contracting companies.

The BIS is also concerned with a long-term negative phenomenon that sees industry sectors regulated by law faced with attempts by regulated industry entities to exert influence over these sectors in order to forward their own specific interests. The entities have long used two methods: firstly, they attempt to influence regulatory and supervisory authorities directly, or secondly, they try to influence the legislative process with regard to proposed regulation.

Even though there was an overall decrease in the activities aiming to influence supervisory authorities in 2021, the work of some authorities was jeopardized by personnel shortages or by a lack of expertise. These shortcomings allowed regulated industry entities to influence the drafting of regulatory legislation by taking advantage of their superiority in terms of expert knowledge. The frequency of these activities was even higher than in the previous year. When pushing forward their interests, the regulated entities very often tried to conceal the origins of the proposed legislation in order to make the proposals look unbiased. This allowed them to justify the proposals by



interests (e.g. lower price rates for the end customers), although in reality, the proposals suited their own aims.

Regulated industry entities were involved in drafting regulatory legislation not only covertly but also in official capacity, e.g. as members of various working groups. Transparent participation of regulated entities is generally viewed as beneficial, however, in specific cases, regulatory legislation was drafted by a very limited group of entities, while the existence of a broad platform for official participation in working groups was only meant to disguise the reality.

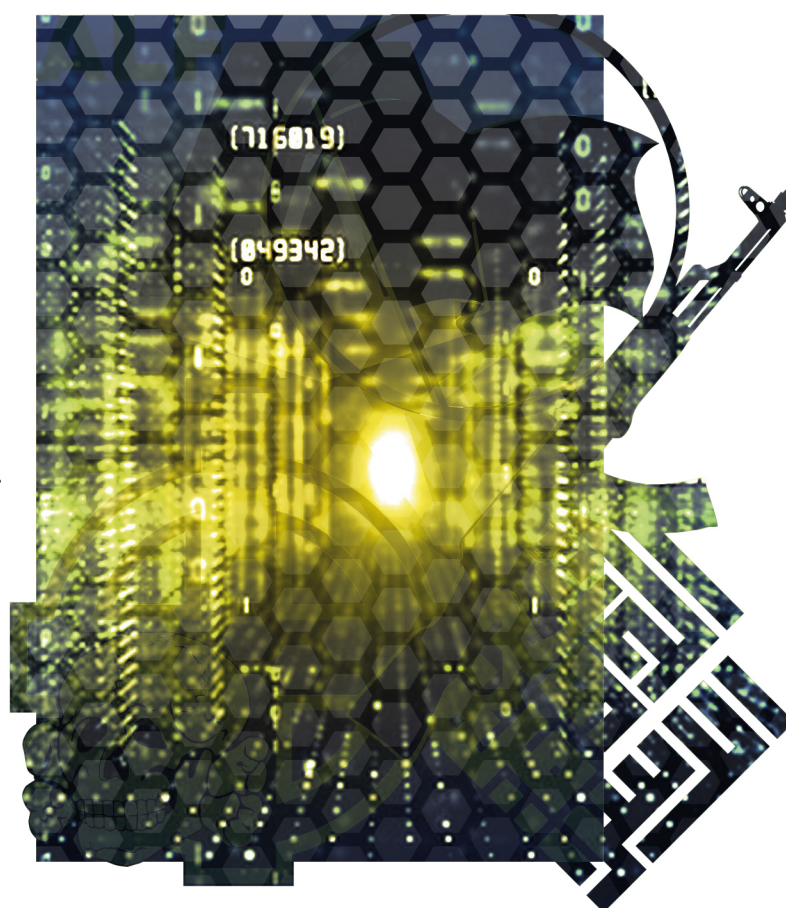
The transfer of expert roles from competent national authorities to regulated industry entities poses significant risks with regard to the energy sector, whose work will probably undergo a complete reconfiguration as new conditions are about to be set for many years in the future due to the Russian invasion of Ukraine.

In several industry sectors, public tenders suffered from the fact that some contractors were given undue favour, leading to embezzlement of public funds and illegal enrichment of those in charge of the tenders. As result of personal ties between representatives of contracting authorities and contractors, contractors were given access to confidential documents or tender requirements were modified to suit contractors' needs, for example. Frequent examples included the procurement of over-priced or needles consultancy, marketing, IT or legal services.

Other negative phenomena linked to public tenders included construction contractors repeatedly abusing their position, as they attempted to curtail their competitors' access to the market or tried to obtain contracts for companies which they had links to in terms of ownership or staff. In some sectors (mainly IT), public bodies struggled with long-term dependency on a specific supplier despite efforts to escape – at least partially – the state of vendor lock-in.

Furthermore, the BIS's attention was brought to the degrading financial situation of some state or state-controlled entities in 2021. This situation was the result of both practical reasons

and failure to follow plans to remedy the situation, past wrongdoings etc. In one particular case, the situation became so urgent that it put at risk the entity's future financing options (e.g. eligibility to obtain credit) or its operations as such. Given the recent economic developments, the standing of some entities might become even more uncertain in the near future.



Violent action, extremism and radicalisation

The main Islamist terrorist organisations, i.e. the Islamic state and Al-Qaeda, continued seeking to launch an attack in the countries of the West. However, their capacity to do so remained limited throughout 2021. That is why they took a pragmatic decision to focus on regional conflicts in Africa and Asia in order to

create a foothold for expanding their terrorist activity worldwide. With regard to the West, the terrorist organisations did not go any further than inciting their supporters to commit unsophisticated attacks. Terrorist propaganda had an impact on some perpetrators of attacks which took place in Europe in 2021. There has been a continuing trend of unsophisticated attacks by lonely attackers with no direct links to terrorist organisations but acting under the influence of their propaganda. The perpetrators often showed signs of mental health issues, making it difficult to determine in certain cases whether the attack was motivated by ideology or whether its primary cause was mental illness. Be it as it may, psychological disorders undermine resilience against manipulative propaganda.

In comparison with the period before the defeat of the Islamic state in March 2019, radicalism was displayed less often in the Czech Republic. This illustrates the degree to which the threat of Islamist terrorism in the Czech Republic was fuelled by the Islamic state's victories and its idealized image created by propaganda. In terms of numbers, there were less than a dozen of individuals showing signs of Islamist radicalisation in 2021 and they were mostly identified due to their suspicious contacts from abroad. There were also some isolated cases of applauding terrorism or sharing jihadist propaganda. The individuals involved originated mostly from Muslim countries – namely the Maghreb region – or they were ethnic Albanians; in one case, the person involved was a Czech convert.

Former Islamic state fighters and their family members coming secretly back to Europe remained a threat in 2021. In this regard, the BIS's attention was brought to a couple of individuals, but the presence of any returnees in the Czech Republic could not be confirmed. Concerning the dozen of individuals with links to the Czech Republic who joined the Islamic or other jihadi organisations in Syria and Iraq state in the past, most of them are deceased or remain missing. The two Czech citizens, who have joined Hayat Tahrir Al Sham, stayed

in the area controlled by this terrorist organisation.

Even though the threat to the Western world posed by Afghanistan increased following the Taliban's takeover, the change of regime had no major impact on security in the Czech Republic. Furthermore, the Afghan community in the Czech Republic did not show any significant support for radical Islamist movements.

Same as in 2020, the Czech Muslim community was strongly affected by the COVID-19 pandemic and related restrictions in 2021. The social and religious life of Muslim organisations, including the operations of individual houses of prayer and mosques or festivities, was paralysed for most of the year because in most cases, official Muslim organisations strictly observed all health-protection measures.

Virtually all official Muslim organisations adopted a very passive stance towards both the public and their followers. Besides that, there were continuing discussions regarding the construction of a new mosque with the help of a foreign organisation under strong Russian influence. On the other hand, there was a decrease in the activity of the Kazakh "Pure Islam" sect.

The Internet continued to be the main communication tool used by Muslims, however, this fact did not provoke an increase in the potential threat of radicalisation among individual members of the Muslim community. The BIS noted only a few isolated accounts on social media which showed interest in groups or personal accounts linked to Islamism. In all these cases, the contacts with Islamists were indirect and of low significance.

The dominant interest of the extremist scene in 2021 was to express opposition against the approach taken to combat the COVID-19 disease. However, extremists showed very little activity in this regard (with the exception of taking part in some protests against COVID-19 related restrictions). Only on sporadic occasions, extremists organised autonomous actions. Furthermore, the contacts between Czech and foreign extremists were limited to the bare minimum

and they were conducted mainly on personal level. Generally, the activities of extremist entities have continued to stagnate. Nevertheless, the BIS assesses that there is a threat in the form of possible self-radicalisation of mentally unstable individuals who for example, could come under the influence of views and information spread by representatives of the extremist, populist or conspiracy scene.

Ideological extremism (neo-Nazism, fascism, communism etc.) has been long losing its position of the main moving force of anti-democratic sentiments. Conversely, individuals and groups with opposing values managed to cooperate, putting their differences aside to some extent in order to “fight against the common enemy”. This trend was boosted by the pandemic crisis. As the pandemic gradually fades away, issues accentuated up by the extremist scene in the past are likely to resurface (migration, racial and gender issues, relations with the EU etc.); however, the importance of ideological extremism will most probably continue to decrease.

Militias in the Czech Republic are represented by a heterogeneous set of diverse groups with loose links between each other. Many of them show some actual activity only on rare occasions and in an uncoordinated manner. The ideological background of individual militia groups has no clear contours and ideology is not the moving force of their existence. Militia members include individuals with staunch anti-establishment views as well as people with no ideological stance who are only interested in militaristic collective activities. Generally, the mind-set of militia members can be described as a mixture of ultra-nationalism, sympathies for authoritarian regimes (mainly the Russian Federation) and general distrust of democracy. Since the beginning of the COVID-19 pandemic, many militia members have been showing strong opposition against the measures introduced by the government in order to limit the spread of the disease as well as against strong opposition against vaccination. With regard to the activities

of the militias, illegal production of firearms and explosives is considered as the greatest threat.

Contacts between Czech and foreign militias are rare and despite proclaimed cooperation, they are based on personal ties between a limited number of individuals.

Protection of Classified Information, Security and Crisis Management

The security of information and communication systems within the BIS focuses mainly on provision of the confidentiality and integrity of information. Moreover, it focuses also on continuous improvement of 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 (NÚKIB). In 2021, the information system for communication among NATO member states' intelligence services was successfully re-certified.

All users of certified information systems are trained in accordance with the Act No. 412/2005 Coll. on the Protection of Classified Information before accessing the systems for the first time and then undergo annual trainings focused on the observance of the security policy of information systems within the BIS and on the raising of awareness regarding the cyber security.

In 2021, no serious security incident was detected within the BIS.

In the domain of cryptographic protection of classified information, preparations for a new

system of classified communication with partner intelligence services were made. On the ground of a NÚKIB's regulation, a recertification of cryptographic protection workplaces was made including updating of their security mechanisms.

In 2021, the BIS detected no serious incidents or disclosure of cryptographic devices. Employees of the cryptographic protection and operators of individual both new and current cryptographic devices have been regularly trained.

In 2021, 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. New mandatory components of the object documentation for BIS workplaces and premises were made and object documentations were revised in order to meet current requirements.

In 2021, ordinary activities regarding physical security were influenced by the construction of a technical and administrative compound. Regulatory measures were taken to secure the perimeter and entry to the compound in order to minimize the disruption of usual activities of the BIS.

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. The committee issued organisational and system decisions or recommendations in order to secure the operation of the BIS and minimize the risks connected with the COVID-19.





Security information service

Cooperation with Czech Intelligence Services and other State Authorities

Cooperation with Intelligence Services of the Czech Republic

In 2021, the BIS provided dozens of intelligence and findings to the Military Intelligence (in Czech: Vojenské zpravodajství – VZ) and the Office for Foreign Relations and Information (in Czech: Úřad pro zahraniční styky a informace – ÚZSI). 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 2021, the BIS cooperated with the Ministry of Defence (in Czech: Ministerstvo obrany – MO) 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 cooperated on trainings of EU/NATO crisis management bodies or on COVID-19 protective measures.

Cooperation with the Police of the Czech Republic

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

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 2021, the BIS provided assessment of 558 578 applications for short-term Uniform Schengen Visa. The number of visa applications has been influenced by the continuing COVID-19 pandemic. Compared with 2020, the number of the applications was a little higher, but still significantly smaller than before the pandemic.

In 2021, the BIS continued to cooperate with the Directorate of the Alien and Border Police (in Czech: Ředitelství služby cizinecké policie – ŘSCP) resulting from the Act No. 49/1997 Coll., on Civil Aviation. The cooperation consists in elimination of security risks posed by natural persons accessing security areas of airports. In 2021, the BIS provided assessments of 4 137 individual applicants for the reliability certificate issued in accordance with the Act on civil Aviation, which was more



than half less than in 2020. The increase of the number of applications in 2020 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. Moreover, the planned amendment of the Act shortening the validity of the certificate was not approved.

The cooperation with the National Centre for Combating Organised Crime of the Criminal Police and Investigation Service (in Czech: Národní centrála proti organizovanému zločinu – NCOZ) took the form of exchange of intelligence on major economic interests, terrorism and cyber security.

Cooperation with other State Authorities and Institutions

The BIS provides chosen state authorities with information and stances regarding se-

curity screening of individuals and companies both based on legal regulations and on interdepartmental cooperation. The National Security Authority (in Czech: Národní bezpečnostní úřad – NBÚ), Ministry of the Interior (in Czech: Ministerstvo vnitra – MV) and Ministry of Foreign Affairs (in Czech: Ministerstvo zahraničních věcí – MZV) 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). Field inquiries involve standard intelligence activities including the use of surveillance equipment and techniques for information gathering.

In 2021, 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 93 natural persons and 3 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.

The Ministry of the Interior and subordinate entities provide 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 2021, the BIS also cooperated with the Ministry of the Interior on vetting of legal and natural persons applying for permits for employment facilitation services. The BIS vetted 1068 natural persons and 629 legal persons.

At the request of the Department for Asylum and Migration Policy of the Ministry of the Interior (in Czech: Odbor azylové a migrační politiky MV – OAMP), the BIS provided assessments of ca. 163 000 applicants for residence permits in 2021. The comparison with 2020 is not applicable, because of a decrease in the number of applicants probably caused by the COVID-19 pandemic in 2020. Compared to previous year, there has been a growing trend in the interest of foreigners in residence permits.

Moreover, at the request of the Department for Asylum and Migration Policy of the Ministry of the Interior (in Czech: Odbor všeobecné správy MV), the BIS provided assessments of 547 applicants for granting or extension of international protection. In 2021, most of the applicants came from Afghanistan owing to political changes and consequent unstable security situation in the country. Other larger groups of applicants came from Syria, Belarus, Ukraine, China, Kazakhstan or Iraq. The BIS also cooperated with the Department for Asylum and Migration Policy on vetting of

individuals within the Medical Humanitarian Programme MEDEVAC. As well as in 2020, the programme was mainly focused on providing help for Belarusian citizens in 2021.

At the request of the General Administration Department of the Ministry of the Interior, the BIS provided assessment of 3585 applicants for Czech citizenship in 2021. The number of applicants for Czech citizenship has not significantly changed compared to 2019 and 2020.

The cooperation with the eGovernment Department of the Ministry of the Interior consists in vetting of applicants for the accreditation to manage qualified electronic identification system. The BIS vetted 2 legal and 27 natural persons. In connection with the upcoming computerization of the state administration, the number of such requests for vetting will increase. This regards e.g. the Amendment of the Act No. 365/2000 Coll. on Public Administration Information Systems and on Amendments to Other Acts, effective from 1 September 2021. The Act enables the Ministry of the Interior to request information from intelligence services and other state bodies on applicants for an entry in the catalogue of cloud computing that is administered by the Ministry of the Interior.

Within the interdepartmental work group "Impacts of the Public Administration Computerization on the Activities of Security Forces in the Czech Republic", the BIS cooperated with the Ministry of the Interior and other involved security forces on measures regarding the computerization of the public administration.

Furthermore, the BIS cooperated with the Security Department of the Ministry of Foreign Affairs. The cooperation consisted in elimination of security risks regarding persons applying for the cooperation with the Ministry. In 2021, the BIS assessed security risks of 652 natural and 56 legal persons; e.g. 25 candidates for honorary consul, 24 applicants for the accreditation for military attaché, 30 applicants for granting or extension of a long-term journalistic accreditation, 95 applicants for a job at an

embassy as local forces and 148 applicants for a working stay at the Ministry of Foreign Affairs or a Czech embassy abroad. Compared to 2020, there was a little increase in the number of the vetted persons.

The Act No. 34/2021 Coll. on the Screening of Foreign Investments and Amendments of Related Acts came into effect in 2021. The main body responsible for the screening of foreign investments is the Ministry of Industry and Trade and the BIS is one of the entities that take part in the screening and provide the Ministry of Industry and Trade with information. The Act establishes rights and duties of foreign investors, whose ultimate beneficial owner is from third countries, in specific fields stipulated by the Act. The aim of the Act is to procure the protection of the security of the Czech Republic and its internal or public order and, at the same time, to increase legal certainty for coming foreign investors by the pre-set regulations of the Act.

Investments and related entities are screened at three levels and the BIS takes part in all of them. The first level consists of notifications of screenings of third country investments in other EU member states and the Czech Republic has an option to comment on them. The second level consists of consultations for investments screened on the ground of the Act or for investments possibly endangering the security of the Czech Republic and its internal or public order, whose investors voluntarily choose to request a screening to obtain legal certainty. The third level consists of procedures that are obligatory for a narrow group of the most sensitive investments with mandatory approval of the state before the transaction. It is also possible to initiate a screening procedure ex officio within five years since the transaction in the event of a negligence on the part of the investor.

Since the date of entry into effect of the Act, the BIS screened 78 legal persons and 54 natural person within European notifications and 57 legal and 69 natural persons within



screening of investments planned in the Czech Republic (consultations and procedures).

The BIS regularly shared intelligence information within the Joint Intelligence Group (in Czech: Společná zpravodajská skupina) and contributed to evaluation of security situation regarding possible danger to the Czech Republic. The BIS has also shared information within the National Contact Point for Terrorism (in Czech: Národní kontaktní bod pro terorismus – NKBT, one of the departments of the National Centre for Combating Organised Crime). 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 2021, the BIS also cooperated intensively with the General Inspection of Security Forces (in Czech: Generální inspekce bezpečnostních sborů – GIBS), Financial Analytical Office (in Czech: Finanční analytický úřad – FAÚ), Customs Administration (in Czech: Celní správa ČR), General Directorate of Customs (in Czech: Generální ředitelství cel), 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 WMD and their carriers and trade in military material. Cooperation was conducted primarily with customs administration bodies both on the level of the Ge-

neral Directorate of Customs and individual customs directorates. The BIS continued to cooperate 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.

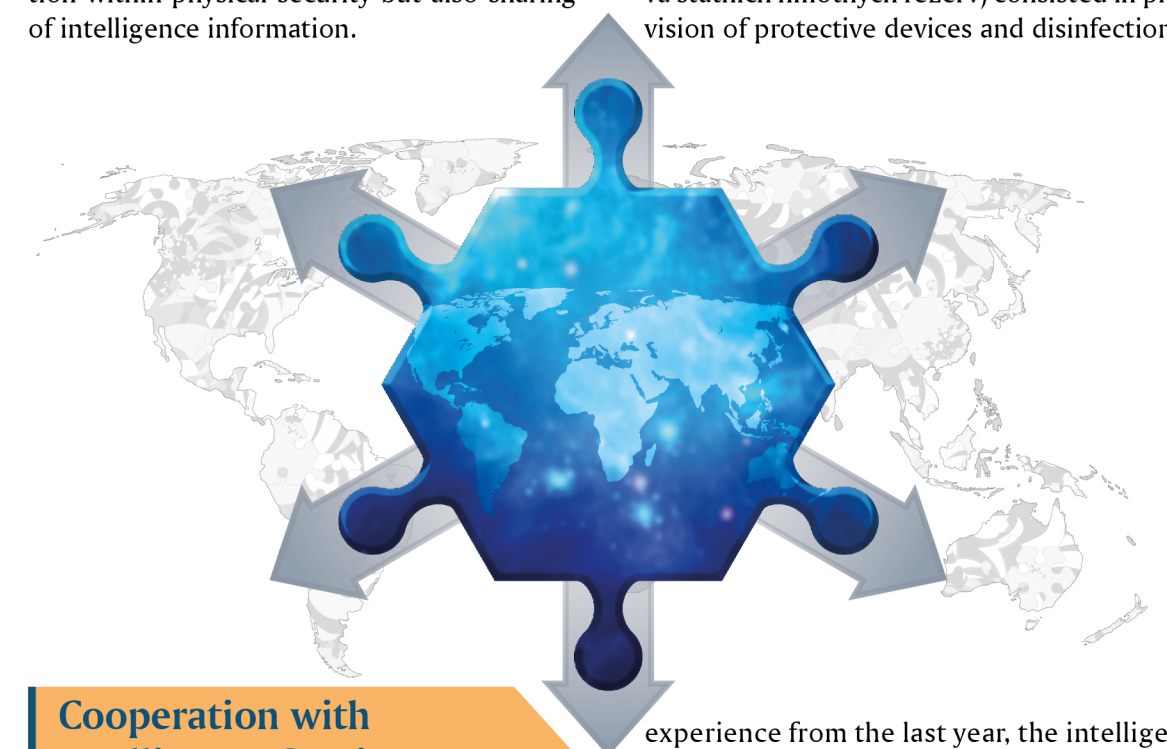
The BIS continued to coordinate a task of the Committee for Intelligence Activity regarding exports of non-controlled items with possible dual-use to high-risk countries. Representatives of the Ministry of the Interior, Ministry of Foreign Affairs, Ministry of Industry and Trade, State Office for Nuclear Safety, General Directorate of Customs, Financial Analytical Office, Office for Foreign Relations and Information and Military Intelligence also took part in the fulfilment of the task.

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 communication with the General Financial Directorate concerned the authorisation of the BIS to gain information from tax proceedings. The BIS also shared information belonging to the scope of their action with prosecuting authorities, the State Office for Nuclear Safety and the Office for the Protection of the Competition (in Czech: Úřad pro ochranu hospodářské soutěže). Moreover, the BIS consulted with executive authorities, mainly with the Ministry of Industry and Trade and Ministry of Interior, regarding prepa-

rations for the construction of a new nuclear source.

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 2021, 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 (in Czech: Správa státních hmotných rezerv) consisted 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 on the basis of the approval of the Government. 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 in 2021 is concerned, the BIS was active in all organizations of which it is a member (e.g. the Counter-Terrorism Group or NATO Civilian Intelligence Committee).

With partial relaxation of anti-pandemic measures in individual states and with the

experience from the last year, the intelligence community adapted the form and way of cooperation, which resulted in a year-on-year increase in meetings. Considering financial efficiency and changeable pandemic situation, also electronic communication means has been used and developed.

In 2021, the BIS received more than 12 000 reports from its foreign partners and sent ca. 2 200 documents. BIS representatives took part in more than 700 international strategic and expert meetings. After an exceptional decrease in 2020, the increasing trend in the number of meetings and shared information has returned. 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 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 the 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 activities of the BIS 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. As regards the BIS, 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 General or by a BIS official designated by the Director General for this purpose; or request due explanation from the BIS Director General should they feel that activities of the BIS illegally violate the rights and freedoms of 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 shall 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. However, 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 an intelligence service can be undertaken only if approved by the Director General 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 20 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, records for the payment of salaries of members or employees of the BIS, 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, observance of vehicles employment and observance of condition and employment of buildings, energy services and compulsory inspections and audits. No severe infringement of regulations was uncovered within these inspections.

The BIS Sickness Insurance Body carried out four inspections of persons temporarily unable to work. And the BIS as the employer carried out one inspection of persons temporarily unable to work within first 14 days of temporary disablement of an employee in an employment relationship. No infringements of regulations were uncovered.

Employees of the archive and of the control group carried out 30 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 2021, 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

Activities of the BIS Inspection Department 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 member; investigation of conduct suspected of having the traits of a misdemeanour and of a disciplinary infraction by a BIS member, including emergencies; investigation of complaints, notifications and motions by the BIS members 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.

Also in 2021, 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 member were referred to a disciplinary proceeding.

One of 157 reports was evaluated as a complaint about conduct of a BIS member. The complaint was found unreasonable. All reports were examined and evaluated and no violations of internal or generally binding legal regulations on the part of a BIS member 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

In 2021, the budget of the BIS was stipulated by the Act No. 600/2020 Coll., on the State Budget of the Czech Republic for 2021. Approved revenues amounted 250 000 thousands CZK and expenditures 2 297 315 thousands CZK.

Besides, the BIS registered claims to unconsumed expenditures. Total budget of expenditures, including employment of claims to unconsumed expenditures, amounted 2 726 655 thousands CZK as of 31 December 2021. Total real expenditures amounted 2 260 154 thousands CZK in 2021.

Service's funds were mainly invested in maintaining of serviceability of the material and technical base and its most necessary development, including the currently most important action, the construction of a technical and administrative compound. Another necessary investment has been allocated to information and communication technologies and intelligence technologies. 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. These expenditures were significantly influenced by the unavailability of several required technologies in the last quarter of 2021.

Payroll expenses traditionally accounted for the majority of regular expenditures, in-

cluding mainly salaries and equipment payments and severance benefits, i.e. payments to retired personnel.

Further regular expenditures were comprised mainly of spending on special equipment and special funds necessary for intelligence activities. Other operational expenditures were e.g. common material expenditures, expenditures for purchase of services and energies necessary for daily operations of the Service, and outsourced services and maintenances of property and compounds of the Service.

Also in 2021, the BIS was constrained to procure protective devices, medical supplies and test kits related to measures taken against COVID-19. However, this unplanned expenditures amounted 1 700 000 CZK, which was not a substantial amount within the total budget of expenditures. Regardless the serious epidemic situation in 2021, the Service's activities were not fundamentally violated also thanks to timely taken preventive and organisational measures.

In 2021, regular expenditures were used regularly and continuously, considering their nature and structure. Measures against COVID-19 valid in 2021 influenced several fields of regular expenditures e.g. for training courses, conferences, and foreign business trips; thus these expenditures were lower than in years before the COVID-19 pandemic.

**Annual Report of the
Security Information Service
for 2021**

Bezpečnostní informační služba
P. O. BOX 1
150 07 Prague 57
Czech Republic
Phone: +420 235 521 400
Fax: +420 235 521 715
E-mail: info@bis.cz
Data box: cx2aize