

ANNUAL
REPORT



2022

**SECURITY
INFORMATION
SERVICE**





**Annual Report
of the Security Information Service
for 2022**

Dear Readers,

You are holding in hands the latest unclassified annual report on the work of the Security Information Service (BIS). This time we are looking back on the year 2022, a year which left a tragic mark in history. On 24 February 2022, Russia launched its attack against Ukraine and set off the greatest armed conflict on European soil since WW2. The brutal and utterly unprovoked aggression disrupted the security landscape of the old continent and dramatically changed the way Russia is looked upon. The threats which the BIS and other intelligence services in democratic countries had been pointing to for several years became a reality. Today, nobody can say that our warnings were groundless or exaggerated.

Unsurprisingly, the conflict in Ukraine had an impact on the life in Czechia. The war exacerbated economic difficulties, energy and fuel prices went up, the inflation skyrocketed and a part of the society begun to show certain signs of radicalization. Negative impacts on the society were at least partially outweighed by key changes in the domain of national security. The until recently overstuffed Russian diplomatic mission to Czechia was scaled down and as a consequence, dozens of Russian diplomats and consular workers stationed in Brno and Karlovy Vary were forced to leave, including individuals with ties to Russian intelligence services. Moreover, a dramatic change took place in the views of Czech political representatives on national security and defense. Czechia's defense budget is being gradually increased by a significant amount and strategic documents on Czechia's defense policy are undergoing important changes.

Our country has become one of the leading and most fervent supporters of Ukraine and the Government was joined in its effort to help the Ukrainian defenders by the private sector and most importantly by individual citizens acting on their own initiative. This fact fills me with immense pride.

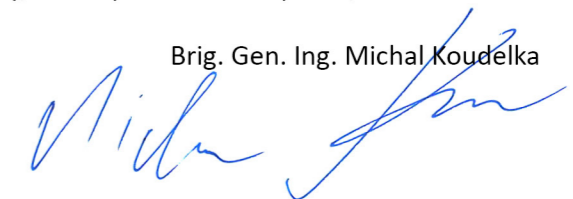
Even though the conflict takes place many miles from our borders, its security implications have had and will continue to have an impact on our country. The BIS has already taken steps to prevent violations of embargoes regarding exportations to Russia. The Service has also been monitoring the potential risk of arms trafficking from the warzone and it has been countering the activities of Russian intelligence services targeted against Czechia. In connection to the war in Ukraine, we have been paying attention to a certain level of gradual radicalization among a part of the Czech society which is under a strong influence of hostile Russian propaganda.

It is only natural that the armed conflict became the foremost security issue. However, the BIS cannot relax its efforts in other areas of its scope of powers nor it can leave aside activities of other foreign intelligence services among which China assumes an increasingly dominating role.

I would like to conclude by expressing my hope that the war in Ukraine will be soon over and that the World, and namely Europe, will learn from it and become even stronger. As usual, the following pages will provide you with a volume of information which despite its general nature should allow you to have a valid insight into the work of the BIS. The information also contains an overview of the issues which the BIS has been investigating and which became the subject of its reports to lawful addressees.

Hoping for your health and safety, I wish you all the very best,

Brig. Gen. Ing. Michal Koudelka



Nature and Scope of Intelligence Activities

The activities, the status and the scope of powers and responsibilities of the 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 legislation.

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 defense of the Czechia. 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 Czechia 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 Czechia's other intelligence services. 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 Activity and Findings

In 2022, the national security of Czechia was greatly impacted by one major event, the Russian invasion of Ukraine, which continues to determine the activity of the BIS in all areas of its scope of powers. The ongoing conflict creates risks to Czechia's security primarily in terms of intelligence activities of foreign powers, energy security, cyberattacks and disinformation.

Right after Russia launched its military campaign against Ukraine, the BIS took active part in shaping and implementing Czechia's security response. Under the new circumstances, a functional national security framework proved to be of crucial importance, being essential for efficient and quick coordination among both security services and other national authorities. The BIS sees cooperation between national authorities as the key element for putting in place sanction mechanisms and drafting legislative changes which would improve the country's capacity to counter aggressive action by hostile states in the future. The activities of the BIS included a security review of residency permits held by individuals with links to the Russian or Belarusian state and investigations into property owned by entities sanctioned by the EU.

In the period of one year since the Russian invasion, several hundreds of thousands of Ukrainians fled their homeland (approx. 75% of them being women and children). Although the number of people fleeing Ukraine continues to decline, the influx of migrants is expected to stay on a very high level due to worsening humanitarian conditions in Ukraine. Despite the massive wave of migrants arriving in Czechia in 2022, the BIS did not note any adverse impact on security. Moreover, the Czech Police did not report any increase in crime in connection to the growing number of refugees from Ukraine.

The BIS also investigated reports by its foreign partners that individuals involved in terrorism (i.e. persons currently listed in terrorist databases in various European countries) have attempted to enter Europe by joining the exodus of refugees from Ukraine. However, these individuals were mostly searched for by the Russian Interpol and had no past links to any EU countries, which meant that European security services had no intelligence on them. It is rare for individuals of clear

security concerns linked to organizations such as the ISIS to hide among refugees. Given that only a marginal number of these cases occurred among the several millions of people who fled from Ukraine, there is no systemic risk involved. Similarly, the BIS investigated the possibility that the wave of migrants from Ukraine could have been exploited by foreign intelligence officers.

Furthermore, some disinformation communicated by pro-Russian entities in 2022 emphasized the risk of arms trafficking from Ukraine to the EU. The disinformation aimed to undermine or even stop the West's military aid to Ukraine by provoking fear of uncontrollable smuggling of weapons from Ukraine to Europe. One of the popular narratives was that arms provided to Ukraine are being systematically misappropriated and subsequently smuggled back to the EU. Concerns regarding arms trafficking are shared by security authorities in Europe, but it should be noted that there are similar security risks in any armed conflict of similar size and they cannot be fully prevented. Throughout 2022, however, the BIS recorded only minor cases of illegal importation of arms and foreign partners documented no major cases of arms trafficking from Ukraine to the EU.

In 2022, Czechia faced economic and social challenges caused by growing energy prices. For national security reasons, the country needs to put an end to its dependence on raw materials from Russia as soon as possible. The current circumstances require a long-term transformation of the energy sector in the EU countries which will lead to society-wide changes.

The Russian invasion of Ukraine was also accompanied by cyberattacks against Czechia and other countries. At the beginning of the war, the National Cyber and Information Security Agency (NÚKIB) uncovered target reconnaissance activity aimed against Czechia,

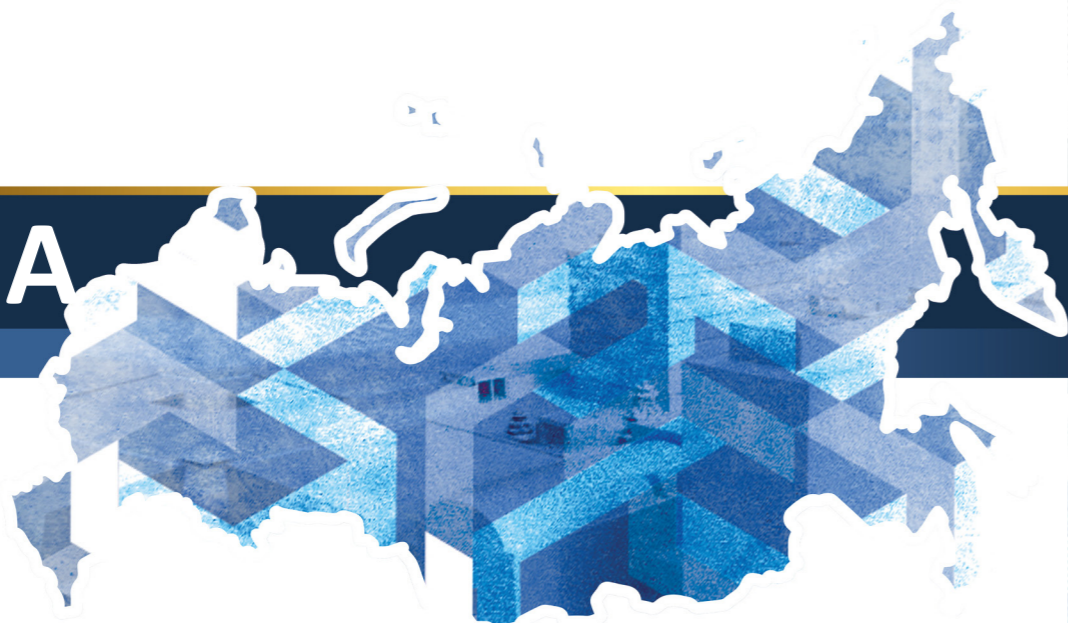
including its public institutions and critical infrastructure. With regard to the war in Ukraine, future cyberattacks will probably be led chiefly against government institutions, media or critical information infrastructure.

Sanctions imposed on Russia by the West play crucial role in reducing Russia's technological and economic resources for future development and in the long term, they are essential for inhibiting its capacity to be a threat to the countries of the West including Czechia. The continuing restrictions and growing demand for sensitive goods will lead to increased efforts to circumvent sanctions and acquire not only military material but also technologies in the broad sense of the term.

In 2022, we saw continuing efforts to project influence by China in both the political and military domain. The Russian invasion of Ukraine fully revealed security threats linked to the dependence of the West including Czechia on supplies of commodities of strategic importance from countries which are hostile to the liberal-democratic social system. In order to gradually eliminate these threats, we will be required to renounce to some extent our own economic growth. It is essential for Czechia to prepare for the new conditions for example by reviewing strategic vulnerabilities with regard to China, searching for alternative business partners and reducing the economy's potential dependency in key sectors. In comparison to Russia, China's capabilities are greater by several orders of magnitude and so would be its leverage (mostly economic) against Czechia.

Even though in 2022, the BIS focused mainly on uncovering the activities of Russia and China, it did not neglect to monitor the undesirable activities of intelligence services from other foreign countries. The BIS therefore noted certain security concerns regarding the activities and interests of the governments of Iran, Vietnam and Azerbaijan in Czechia.

RUSSIA



The Greatest Current Security Threat

In response to the Russian invasion of Ukraine, further reduction of the Russian diplomatic mission to Czechia took place in 2022. Both Russian consulates were closed and despite the already limited number of accredited Russian diplomats in Czechia, a high-ranking diplomat from the Russian embassy was expelled. By this action, Czechia joined the international initiative which led to the expulsion of several hundreds of Russian diplomats and members of administrative-technical staff. To a large extent, these individuals worked for the Russian intelligence services and used their official missions as cover for intelligence activities.

Intelligence officers stationed at Russian diplomatic missions are crucial for Moscow, since diplomatic accreditation provides them with protection in accordance with the Vienna convention on diplomatic relations. Russia's scaled-down diplomatic mission to Czechia therefore had limited capacity to exploit diplomatic posts for intelligence purposes in 2022. Additionally, Russian intelligence officers under diplomatic cover faced adverse reactions provoked by the opposition of the majority of the Czech society against the invasion of Ukraine.

However, the risk posed by hostile activity of actors with other than diplomatic cover has been growing. Nevertheless, the cultivation of personal contacts with human sources became

increasingly difficult for Russian intelligence services in many EU countries in 2022 which is why they have begun to move their activities to other countries. The activities included efforts to gather information on Czechia and recruit collaborators with the aim of spying on EU institutions.

The objectives of Russian intelligence services include monitoring and countering activities of Russian opposition in exile such as conferences hosted by non-governmental organizations and academic institutions attended by representatives of anti-Kremlin opposition. In the course of 2022, the BIS acquired information on the activities of an individual who has been suspected of links to the GRU intelligence service and has repeatedly visited Czechia. On the Czech soil, the individual frequented persons who probably were of interest to the Russian intelligence services. Working under journalist cover, the individual attended international events hosting prominent representatives of the Russian opposition.

The threat of Russian intelligence activity against opposition representatives has become increasingly urgent in the context of the war in Ukraine. However, uncovering Russian activities is an extremely complex task since the Russian intelligence officers and their collaborators maintain a high level of secrecy while on the other hand, the Czech academia



frequented by the Russian opposition can be regarded as a generally unsuspecting environment.

Another area impacted by the invasion of Ukraine has been the pro-Russian milieu. At the beginning, there was almost no support for Russia among the general public due to the fact that pro-Russian activists showed only a minimum of activity. Later, some of Russia's supporters hardened their views or even became radicalized. They actively spread narratives aligned with the stance of Russian propaganda and made contact with other anti-establishment actors. Pro-Russian narratives combined with other public issues resulted in anti-government demonstrations in the second half of 2022 in which some of the pro-Russian activists took part.

The demonstrations eventually attracted Russia's attention. This confirmed that Russia often tries to stoke existing tensions in societies in order to support its interests. Anti-government protests became a subject of Russian domestic propaganda which offered strongly biased coverage. In specific cases, Russia used its supporters to turn the demonstrations into a vehicle for its own agenda in the information space of the EU.

Even though pro-Russian activists attended much fewer commemoratives events in Russia than in the previous year, some of them made a trip to the annexed Crimea in the summer of 2022. Events of this kind as well as interviews

with various individuals from Czechia in Russian media are exploited by Russian domestic propaganda.

Additionally, the conflict in Ukraine had had an impact on organized crime groups from Russian-speaking countries, providing them with new opportunities. Some of these groups in Czechia have links to Russian intelligence services and the war in Ukraine therefore enhances the risk of the groups being directly involved in subversive action or providing mostly material support. The organized crime groups have also attempted to exploit Czechia for laundering financial assets from Ukraine or Russia. Their illegitimate or illegal activities most probably involve money laundering as well as sanctions evasion and legalization of residence.

Following the attack against Ukraine in February 2022, the EU strengthened its measures against Russia, whose military-industrial complex has long had difficulties acquiring certain commodities. Russian entities and their partners were forced to search for alternative routes in order to obtain a much larger range of sensitive goods than before. The BIS has detected efforts to import machine tools, including spare parts, and chemical substances via a number of third countries. Available information shows that the strengthened EU restrictions strongly reduced Russia's access to materials used in military-industrial production.

Geopolitical changes affected also the Czech cyberspace. In 2022, the BIS noted a slight decrease in cyberespionage activity of Russian state / state-sponsored actors against targets in Czechia. A part of the Russian cyber-resources were apparently engaged against Ukraine or other targets. The decrease in attacks by professional hackers was, however, counterbalanced by attacks led by Russian hacktivists.

Russia has continued its efforts to gather information regarding international relations, which include continuous or repeated cyberespionage campaigns. The targets are mainly ministries of foreign affairs, embassies, think-tanks and international institutions. Last year was no different as soon after the invasion of Ukraine, renewed activity of a Russian state / state-sponsored cyber actor, which had come to the attention of the BIS already in the past, became apparent. The actor in question exploited the Czech IT infrastructure for phishing attacks which were clearly linked to the war in Ukraine. The same connection was detected in another cyberespionage campaign which hit – among other targets – organizations providing aid to Ukrainian refugees.

Major cybersecurity incidents in 2022 included a cyberespionage campaign of virtually global scale which focused on international relations and diplomacy. The campaign's intensity was extremely high. For a short period of time, the perpetrators managed

to compromise – among other things – several individual e-mail accounts at the official domain of a Czech government institution and then used the accounts to send out malicious messages.

The partial decrease in Russian cyberespionage activities against Czechia was outweighed by unprecedented increase in attacks by Russian hacktivist groups. Throughout 2022, groups acting in support of Russia's official policies claimed and conducted attacks against Czech institutions and businesses in retaliation for Czechia's support to Ukraine.

Their activity mainly took the form of DDoS attacks. It should be noted that pro-Kremlin hacktivist cyberattacks against Czechia were inexistent prior to the invasion of Ukraine. Similar to other countries, these were opportunist attacks aiming to disrupt the functioning of web servers by extensive quantities of requests. The affected websites belonged to government institutions, telecommunication and transport infrastructure operators, media etc.

The duration and geographical scope of the attacks was limited and their impact on the work of the targeted organizations was marginal. However, the attacks received a great deal of attention in the media, appearing disproportionately significant and thus fulfilling the aims of Russian information warfare as it was perhaps intended in the first place.

E Energy Security

The ongoing war in Ukraine has been an important factor in the domain of national economic interests. It was the energy sector which was the most affected by the war's consequences among which the principal threat was possible outage in supplies of key feedstock, e.g. oil, oil products, natural gas and in the long term nuclear fuel, too. Potential supply outage would have far-reaching consequences for large fields of domestic economy which is why it was essential to look for alternative suppliers and supply routes. Government institutions and state-controlled entities were able to find solutions and implemented or at least initiated several key projects which will lead to more secure supplies in the future. Simultaneously, the dependence on supplies from Russia has been reduced in reaction to the fact that Russia systematically used energy supplies as leverage when promoting its geopolitical interests.

Simultaneously, the risk of energy feedstock shortages raised interest among various private entities which attempted to exploit the situation to their own benefit. One thing which their activities had in common was the promise of seemingly advantageous deals on supplies of motor fuels or natural gas. However, there were numerous reasons why the deals in question could not effectively improve Czechia's energy security. In fact, the background of these offers was often clearly suspicious and in some cases, it was assessed that the middlemen involved were employed by Russian entities. On top of that, there were concerns regarding some of the deals that they could not be ever fulfilled.

In the energy sector, regulated industry entities continued to pursue their particular interests. In connection to the war in Ukraine, new legislation needed to be adopted in a very short time, which gave space to covert lobbying and gave private entities the opportunity to influence the creation of legislation for long future periods. In order to promote their interests, private entities often took advantage of their superiority over government institutions in terms of resources or exploited privileged access to certain government representatives with the aim to obtain undue favor when applying for government subsidies.

CHINA

A Complex Threat to Czechia

Officers of Chinese intelligence services continued to develop contacts with Czech political representatives throughout the entire political scene in 2022. At the same time, China has been involving members of the Chinese diaspora with growing intensity in promoting Chinese interests and gathering information, making the diaspora one of the tools of influence operations. The aim of intelligence officers and party officials is mainly to influence public opinion in order to promote a positive image of China. They also make use of previously established collaboration with certain entities in the Czech media sector.

China continued its efforts to counter activities linked to issues known as the Five Poisons, most importantly Taiwan and Tibet, which hold a crucial position in the political agenda of the Communist party of China and are intrinsically linked to the One-China policy. China strongly objected to any collaboration with Taiwan and repeatedly issued government

statements in order to draw attention to violations of so-called red lines. The BIS views such statements as an attempt to discourage any further reinforcement of the relations between Czechia and Taiwan.

Regarding the Chinese diaspora, the BIS also detected the activity of so-called overseas police station employed by the Chinese regime to spy on representatives of Chinese communities in foreign countries. The stations are the long arm of the Chinese regime in relation to Chinese expatriates and in extreme cases, they can be involved in forced repatriations. The activities of Chinese overseas police stations in Czechia, however, have not yet been linked to any illegal aspects or security concerns.

The Chinese continued to cultivate relations with certain representatives of the Czech academia in order to use their knowledge for gathering information on political issues. Such activities pose the risk of seemingly unproblematic research collaboration being

exploited for intelligence and propaganda objectives. Particularly concerning are visits by Czech scientists to China, where even without being aware of it, they can be recruited by intelligence services which often prefer to establish contact with their sources on Chinese soil. There is also a risk in the use of Chinese technology by entities of strategic importance, especially by those involved with critical infrastructure.

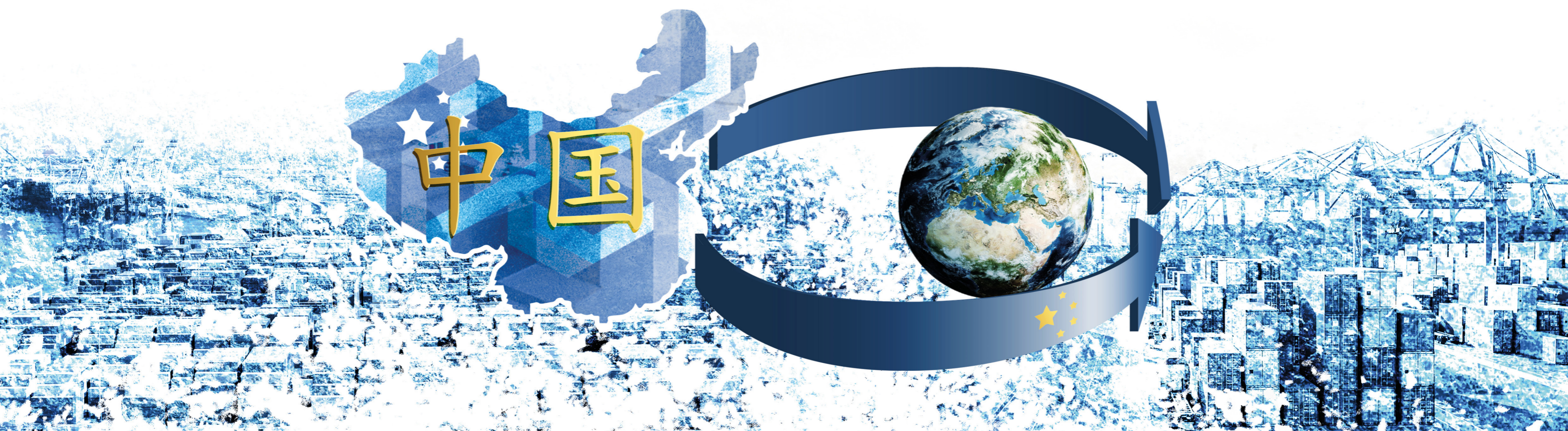
Furthermore, China represents a threat to Czechia in terms of trade in sensitive goods including EDT (emerging and disruptive technologies), know-how transfer and reverse engineering. In 2022, China showed again an interest in companies, goods and know-how which could facilitate its technological research or enhance its research capacities. These objectives are in fact followed by China's policies such as Civil-Military Fusion, Made in China 2025 and China Standard 2035. The BIS's attention was drawn primarily to efforts to acquire producers of aeronautical equipment or electron microscopes, which can be used for the production of microchips.

The Russian invasion of Ukraine prompted China to increase its interest in Europe and

to boost its cyberespionage activities in the region. In Czechia, these efforts took the form of spear-phishing attacks for example, which in some cases targeted government institutions. The attackers then took advantage of some of these institutions in an attempt to impersonate their employees and representatives.

The attacks took place in several waves during which the attackers were trying to exploit the latest political issues of that time. Over the time, the attacks grew in their level of sophistication and the number of targets decreased in a way that on some occasions only a single person was targeted. The incidents took the form of standard cyberattacks in which the attacker – using social engineering – attempts to gain the trust of the victim by impersonating a person whose name the victim is surely familiar with.

The increased cyberespionage threat applied also to Czechia's EU Council presidency during which time Czechia became a target of increased importance to attackers looking for valuable information. That is why the BIS detected growing activity among Chinese cyber actors in the first half of 2022. Some of these activities were at least partially successful.



Disinformation and Conspiracy

The war in Ukraine became the most common subject of disinformation narratives. Following the invasion, the COVID-19 pandemic ceased to be a major topic in the media and the Czech disinformation scene fully refocused on providing support to the actions of Russia. The disinformation scene eventually revived issues which it used to be committed to when it first emerged (i.e. support to Russia and resentment towards the USA, EU and NATO). Given the very limited number of pro-Russia oriented Czech citizens, the disinformers focused on linking the war in Ukraine to sensitive social issues (e.g. growing energy and food prices, financial and material aid to Ukrainian refugees). A recurrent theme which appeared on most disinformation websites was the supposed “ukrainisation” of Czechia. According to this narrative,

the government has focused on helping Ukrainians while leaving the needs of Czech citizens aside. Disinformers aimed to appeal to as broad section of the society as possible by claiming Czechia is a non-sovereign state whose government acts in the interests of foreign countries and foreign citizens.

The activity on the disinformation scene suffered a short-term decrease as result of legal action taken by private entities against some of the disinformation hubs. The scene however quickly adapted to the new situation and managed to keep its audience so that in the course of the year, many of the previously restricted websites bounced back to the original numbers of readers. In fact, a certain part of the population has accepted these websites as their regular source of information.

Synthetic Media

In 2022, AI-based tools for the production of synthetic content in all multimedia forms, i.e. synthetic video (deepfake), images, audio (human voice) and text, became increasingly accessible to the general public.

There is a wide range of legitimate uses for synthetic media, e.g. they are used in the entertainment industry or for educational purposes. At the same time, they can be exploited for crime, disinformation or so-called prank-calls, i.e. to impersonate individuals in order to elicit information or ridicule the interlocutor. Additionally, the Russian invasion of Ukraine has brought about the first use of synthetic media for war purposes (a deepfake video of president Zelensky). However, its potential negative impact was mitigated by a quick counter-action.

The harmful potential of synthetic information is multiplied by its automated dissemination in the information space by the means of social media or comment sections on

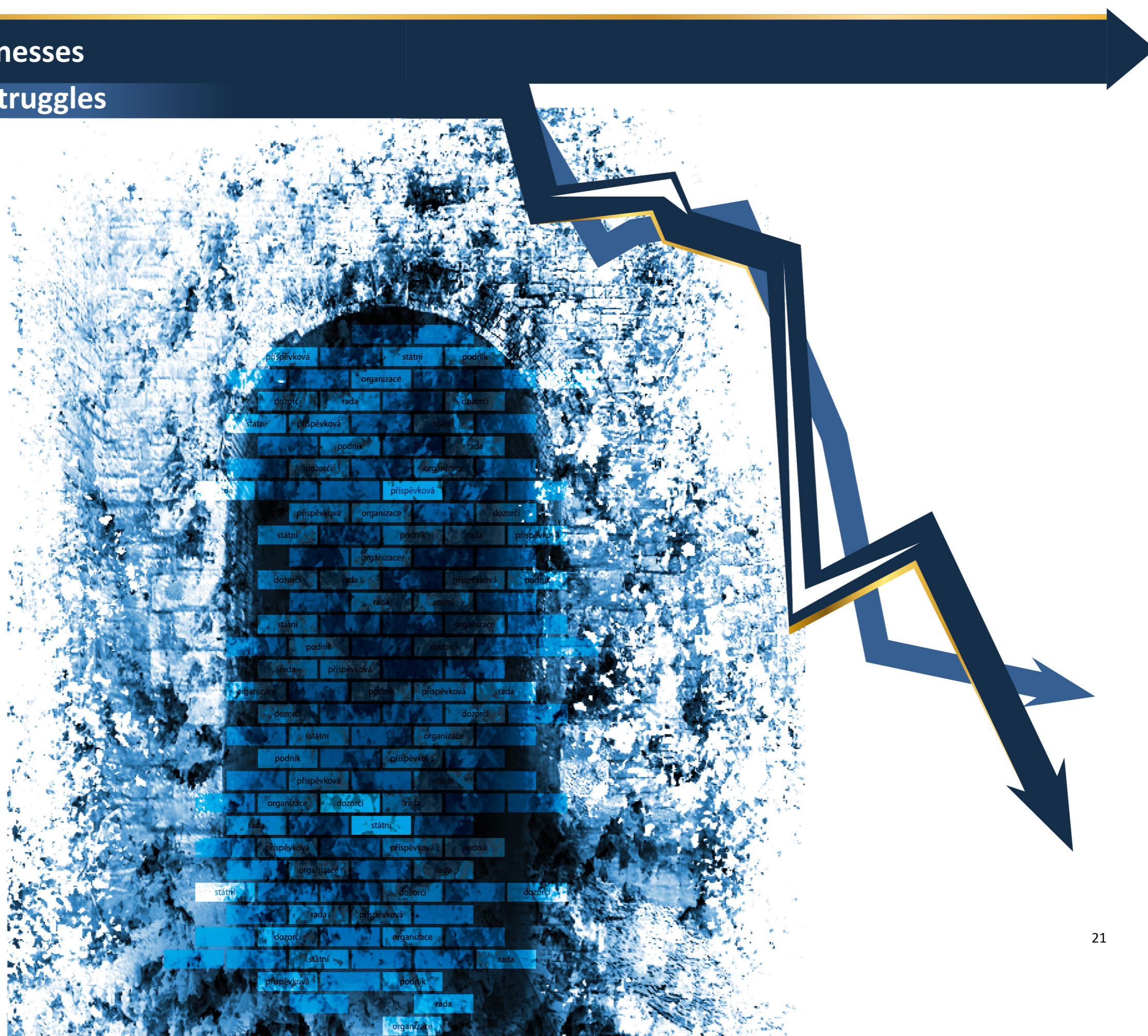
news websites for example. The BIS assesses that the most easily exploitable is the synthetic text as it can be used to generate an infinite volume of content variations with the same message and to flood the information space with a specific agenda. Moreover, synthetic text is significantly cheaper to produce and more difficult to detect than fake audio-visual content.

The existence and development of synthetic media alone will make it possible to dispute the existence of any event, statement or evidence and claim they are a fabrication. The risk is enhanced by the limited resources for quick and automated detection of artificial voice, video or text. The exploitation of synthetic media on a mass scale has been so far prevented by the technical limitations of widely accessible tools. However, these limitations will not last long and the exploitation of synthetic media will be present in the information space with growing intensity.

State-Controlled Businesses and Their Economic Struggles

In accordance with the BIS's prediction, the unfavorable economic situation of certain state or state-controlled businesses continued to deteriorate in 2022. This was to a large extent the outcome of the general economic situation which led to high inflation and interest rates. The situation impacted not only the expenditures of the businesses in question but also the cost of debt funding. In some cases, the economic standing of the businesses did not correspond to official management reports and directors of some of the businesses attempted to distort and manipulate information on the actual economic outcomes in order to make them appear in a more positive light to outsiders as well as to supervisory bodies.

The shortcomings in the information provided to supervisory bodies of state-controlled businesses is a long-term and recurrent issue. It is not only the economic outcomes that are concerned – although they have become the most prominent issue due to the current economic developments – but also other affairs under the scope of powers of supervisory bodies. Members of these bodies often miss adequate, complete and timely information regarding the management of the businesses in question and they are therefore unable to use their powers to ensure lawful and efficient business operations.



Threat of Religious Terrorism

The so-called Islamic state and Al-Qaeda terrorist organizations pursue their efforts to launch attacks on European soil, however, they lack the necessary resources. Islamic State focused on reconstituting its forces, mainly by helping its fighters to escape from Syrian prisons and by supporting the expansion of its offshoots in Afghanistan and Africa. Similarly, Al-Qaeda and its proxy groups prioritized their operations on the African continent. The Russian invasion of Ukraine had a marginal impact on the threat of Islamist terrorism. In Czechia, no Islamist radicals were detected among refugees from Ukraine.

There were only a few successful terrorist attacks motivated by Islamist ideology in Europe in 2022, one of the reasons being that in some of these cases, intelligence services uncovered the preparations. The greatest threat was represented by lone-acting attackers radicalized by online propaganda. In these cases, mental health issues played an important role, too, which is a trend that became apparent already in 2021. Conversely, the importance of adherence to a specific

terrorist organization or ideology decreased. Individuals of security concern have been creating their own ideologies and world-views.

The risk of Islamist terrorism has remained low in Czechia. Signs of radicalization among individuals living in Czechia continued to decline. On the other hand, there was an increase in the number of individuals of security concern staying in the country for a short-period of time, e.g. immigrants from the Middle East. None of these individuals, however, has settled in Czechia permanently. The increase in transit migration was caused by mass departures of Syrian refugees from Turkey. Due to the high numbers of migrants, the capacity of security forces to detect individuals of security concerns decreased.

In 2022, there was no development in relation to Czech citizens who joined the jihad in Syria – they all remained in the Idlib province. Concerning the individuals with ties to Czechia who joined jihadi organization in Syria and Iraq, no new information was obtained. This means that five of them are presumed dead and the others remain missing.

Czech Muslims gradually restored their social and religious activities after the COVID-19 pandemic. However, official Muslim organization in Czechia retain their passive stance towards the public. The Muslim community in Czechia remains moderate in

its nature and the risk of its radicalization has been low. The BIS's attention was drawn to only a few individuals who came in contact with supporters of a radical conception of Islam. None of these contacts, however, represented a threat to Czechia.

Czech Muslims adopted varying stances on the war in Ukraine (just like the majority population). They did not show their views in public due to negative experience from the time before the COVID-19 pandemic when a part of the society viewed Muslims as the greatest security threat. The whole Muslim community felt strongly about the Czech population's fundamentally different approach to refugees from Ukraine and Muslim countries. On top of that, an international Muslim organization, which used to have a Czech branch and was known to be under strong Russian influence, lost its credibility as a result of its open support to the Russian aggression.

The war in Ukraine also led to more intensive military cooperation between Russia and Iran, which has maintained its intelligence presence in Czechia. Anti-government demonstrations in Iran in 2022 incited the local regime to further repressions against its alleged enemies. That is why Iran launches targeted killings throughout the world or lures individuals of interest to countries where they can be kidnapped. The persons put at risk by Iran are members of the Iranian opposition as well as representatives of independent media, including Radio Farda of the Prague-based RFE/RL. On top of that, Iran represents a threat due to its efforts to circumvent international economic and arms sanctions in addition to its recent increased cooperation with Russia.

Traditional Forms of Political Extremism

The BIS detected no act of terrorist or serious criminal nature. The extremist scene is undergoing a period of stagnation and as a whole, it does not represent an important security threat. Following the Russian invasion of Ukraine, the activities of far-right extremists focused on supporting their Ukrainian counterparts. A few right-wing extremists left for Ukraine where they were mostly undertook in tasks in the rear of the zone of combat. A small number of extremists (mainly politically motivated organized right-wing extremists) supported Russia in the war against Ukraine, however, their support only took the form of verbal declarations, having no impact on the security of Czechia.

Even though communism-oriented left-wing extremists sympathize with Putin's Russia due to its authoritarianism and a number of shared viewpoints (e.g. hostility towards NATO and EU), only Russia's most staunch supporters dared to openly express their support. The rest of the left-wing extremist scene showed caution in their statements. Anarchist activists organized several small gatherings and collected donated material to support Ukrainian anarchists. Meetings among left-wing anarchists were rare and in comparison to the past, there were fewer gatherings, benefit concerts or commemorative events.

Paramilitary Groups and Militias

Militias still represent a non-coherent movement which brings together individuals with similar mentality and views on society. Only a few of the militia groups showed real activity. Their activities had autonomous character and the groups were virtually independent of any superior authority. The militiamen have grown in their susceptibility to various conspiracy theories and partially in reaction to the war in Ukraine,

most of them have become admirers of Putin's Russia.

In paramilitary and militia groups, efforts to acquire firearms have been a growing trend. For the time being, available information does not suggest that any of the militiamen would have the intention to use the weapons to commit violent crime. Nevertheless, the threat persists, mainly among militia members suffering from mental health conditions.

Protection of Classified Information, Security and Crisis Management

The security of information and communication systems within the BIS protect primarily the confidentiality and integrity of information. Information systems – both classified and unclassified – are based on advanced technology for information protection. All BIS classified information systems are certified by the National Cyber and Information Security Agency (NÚKIB). In 2022, secret-level classified information systems were 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 which aim to promote the observance of security policies for information systems within the BIS and to raise cyber security awareness.

In 2022, no major security incident took place nor was a cryptographic system compromised within the BIS. Periodic inspections of areas under cryptographic protection and inspections of cryptographic equipment did not identify any shortcomings in management and use nor any violation of security protocol. Cryptographic protection officers and operators of both new and current cryptographic devices undergo periodic training.

In the course of the year, physical security policies were inspected and security protocols and documentation regarding BIS facilities were brought up to date. Additionally, compliance with workplace security protocol was inspected on repeated occasions.

Throughout 2022, physical security management was affected by construction works on a new technical and administrative

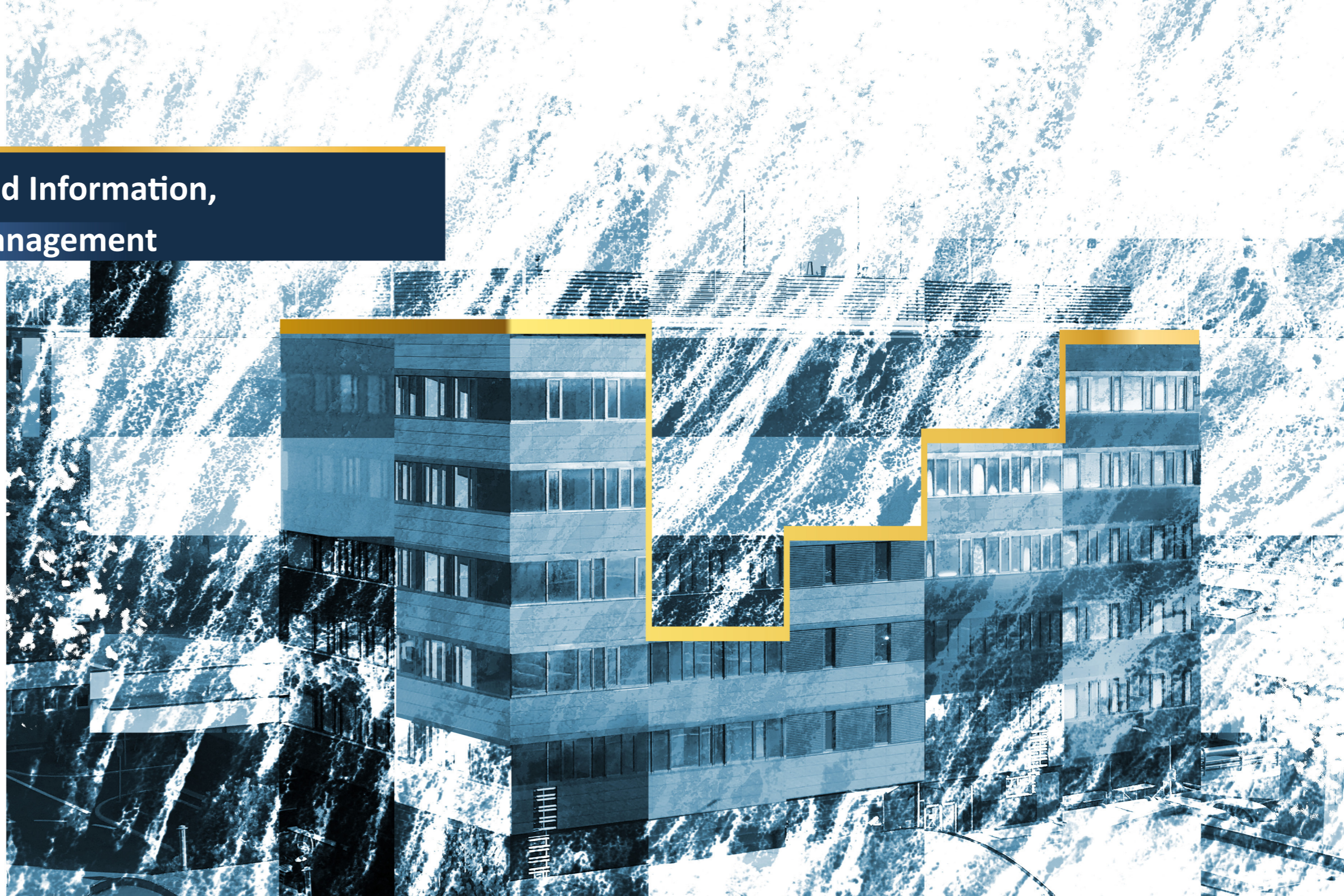
compound. Security measures were taken to secure the perimeter and entry to the construction site in a way that would pose the least disruption to regular activities of the BIS.

In terms of emergency protection of classified information, security policies for BIS facilities

have been updated. The BIS being a part of national critical infrastructure, its crisis policies were updated in accordance with the Act No. 240/2000 Coll. on the Crisis Management.

The crisis committee to the BIS Director General assumed its functions

and conducted regular sittings. The committee issued organizational and systemic decisions or recommendations in order to secure the activities of the BIS while minimizing the risks linked to the COVID-19 disease.



Cooperation with Czech Intelligence Services and Other Authorities

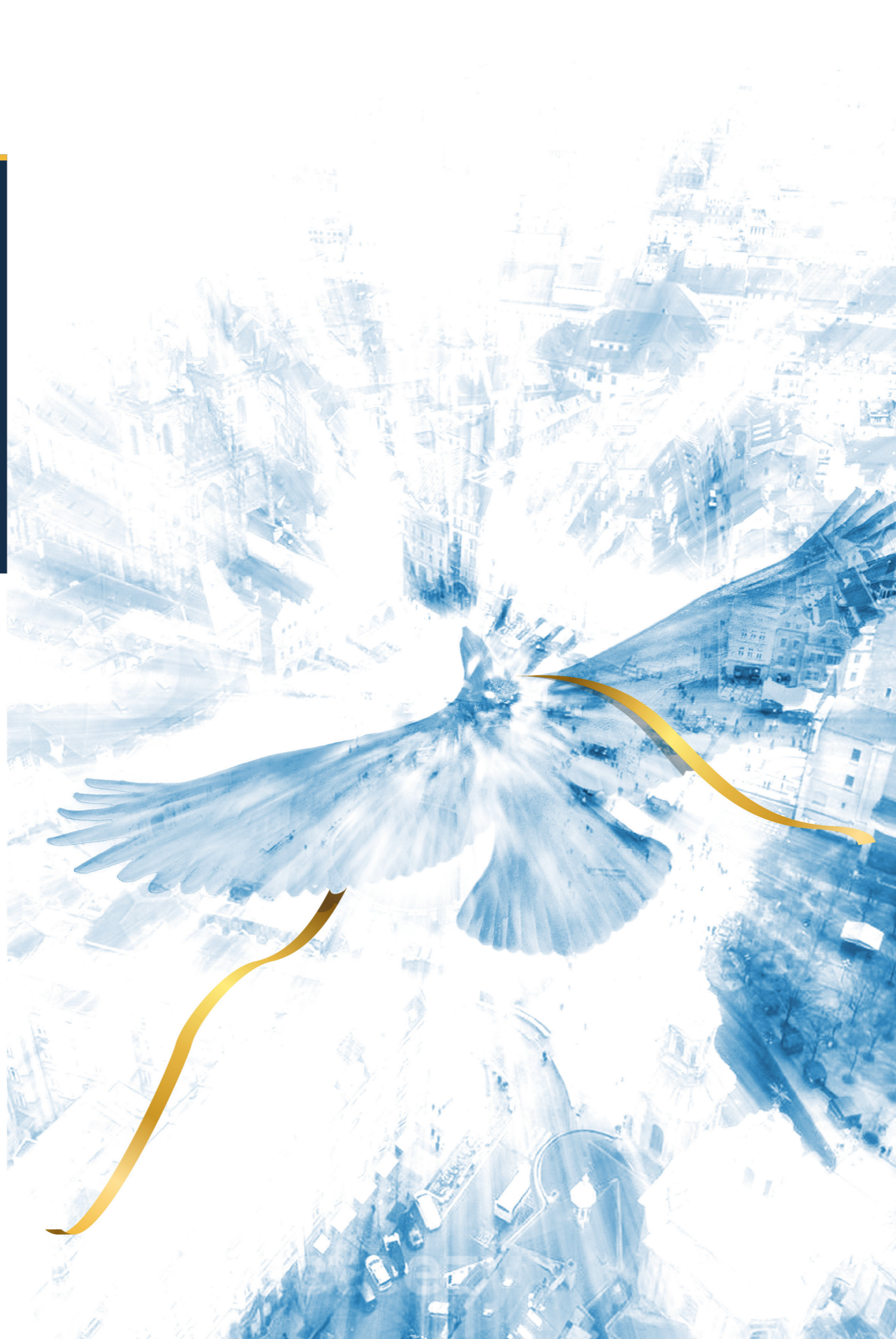
Cooperation with Intelligence Services of the Czech Republic

In 2022, the BIS provided almost 100 intelligence reports to the Office for Foreign Relations and Information (ÚZSI) and more than 40 reports to the Military Intelligence (VZ). Cooperation with both services has taken place on different levels with regard to operational, analytical as well as technical issues.

The BIS continued its cooperation with the ÚZSI on background checks regarding individuals applying for accreditations as diplomats or civilian personnel at foreign diplomatic missions. In total, 168 individuals, i.e. 129 diplomats and 39 members of their families, were screened. In reaction to the outbreak of war in Ukraine and given the decision taken in 2021 to bring the staffs at embassies of Czechia to Russia and Russia to Czechia to equal numbers, there was a clear decrease in the number of accreditation applications by Russian diplomats. While the BIS screened 18 applicants in 2018, there were only 6 of them in 2022.

Additionally, the BIS also collaborated with the Ministry of Defense, i.e. namely with the VZ, on the development of a specialized information system adapted to the needs of intelligence services.

The BIS, VZ and ÚZSI continued their cooperation on providing training to authorities involved in the EU and NATO crisis management systems.



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., it also provides information to the Police of the Czech Republic on condition that important intelligence interests of the BIS will not be compromised. In many cases, cooperation between various departments of the BIS and the Police draws on the nature of the acquired information. Pertaining to specific criminal proceedings, information is also provided upon request to the Police or the public prosecutor's office.

In 2022, the collaboration with the Police took a new dimension when the BIS and the Police's Criminal Police and Investigation Service (ÚSKPV) collaborated on protecting national security during Czechia's presidency to the EU Council (CZ PRES 2022).

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 2022, the BIS provided assessment on 1 076 271 applications for short-term Uniform Schengen Visas. The number of visa applications has doubled as result of the COVID-19 pandemic restrictions having been lifted. Another factor which influenced the Czech visa policy and subsequently the number of screened applications was the war in Ukraine which led to severe restrictions on travel from Russia and Belarus.

The BIS continued its involvement in the screening of applicants for eligibility certificates as demanded by the Act No. 49/1997 Coll., on Civil Aviation. The screening procedure aims to prevent access to protected airport facilities by individuals of security concern. In 2022, 5 761

applicants were screened and in comparison to 2021, there was only a slight increase in the number of applications.

Cooperation with the National Centre for Combating Organized Crime of the Criminal Police and Investigation Service (NCOZ) took the form of exchange of intelligence on major economic interests, terrorism and cyber security.

On top of that, the BIS joined the Police's criminal investigation department (ÚSKPV) in providing security to certain events during Czech presidency to the EU Council in Czechia and in Brussels. The BIS screened 22 424 individuals, including interpreters, chauffeurs, liaison officers as well as administrative and service staff.

Cooperation with other State Authorities and Institutions

The BIS provides several state authorities with information and assessments regarding security screening of individuals and companies based both on legal regulations and on interdepartmental cooperation. The National Security Authority (NBÚ), Ministry of the Interior and Ministry of Foreign Affairs are among the most frequent addressees of such 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 field enquiries 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 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 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 any relevant information without delay, if this does not jeopardize an important intelligence interest of the Service.

In 2022, the BIS conducted more than 20 000 investigations in registers based on the National Security Authority's requests. Following field enquiries, the BIS provided assessments on 111 natural persons and 2 legal persons.

As a member of the interdepartmental work group on the computerization of public administration and its impacts on security forces, the BIS closely collaborated with the Ministry of Interior and other security forces involved on adopting necessary measures.

The Ministry of the Interior and other entities financed by the ministry provide the BIS with a range of services regarding electronic communications, fire prevention, health and safety protection, energy supplies, water management, protection of the environment and catering services.

The BIS also cooperated with the Ministry of the Interior on the screening of legal and natural persons applying for employment agency certification. In 2022, the BIS vetted 552 legal persons and 1 038 natural persons.

Following the outbreak of war in Ukraine, the BIS joined the Ministry in the screening of persons applying for authorization to serve in the Ukrainian armed forces as requested by the Conscription Act. The BIS screened several hundreds of applicants intending to join foreign armed forces.

In 2022, the BIS reviewed the demands of 734 applicants for the renewal of their asylum status. The profile of applicants has changed as result of the new security conditions in Europe caused by the war in Ukraine. Most applicants for asylum were from Ukraine and the remaining mostly from Syria, Belarus and Afghanistan.

The BIS issued reviewed the demands of 149 thousand of applicants for residence permits and 185 thousand of applicants for temporary protection (aged 15 or more). The war in Ukraine had an impact mainly on immigration from Ukraine and therefore on applications for temporary protection. The BIS continued to cooperate with the Department for Asylum and Migration Policy of the Ministry of the Interior (OAMP) on screening individuals involved in the MEDEVAC medical and humanitarian aid program. In total, 12 medical workers who applied for specialized internships in Czechia were screened.

Additionally, the BIS reviewed the application of 5 120 individuals for Czech citizenship. The number of applicants went up by 34% in comparison to 2021.

On demand of the eGovernment department of the Ministry of the Interior, the BIS reviewed 4 applicants for authorization to manage certified electronic identification systems. This included the screening of 8 legal and 44 natural persons. In connection to changes in the Act on Public Administration Information Systems, effective from 1 September 2021, the BIS has begun reviewing applications to the cloud computing register which is administered by a specialized section of the eGovernment department. In the course of 2022, the BIS reviews 59 applications and screened 67 legal and 155 natural persons.

Furthermore, the BIS cooperated with the security department of the Ministry of Foreign Affairs. The cooperation involves the screening of persons applying to work for the Ministry. In 2022, the BIS screened 542 natural and 22 legal persons. The applicants were future honorary consuls, military attachés, accredited journalists or foreign workforce at Czech diplomatic missions. However, the greatest portion of applicants applied for internships at the Ministry or at a Czech diplomatic mission abroad.

Cooperation with Foreign Intelligence Services

In several domains within the scope of powers of the BIS, cooperation with intelligence services of foreign countries plays a vital role in the BIS's effort to gather key information regarding the national security. On the basis of the Government's approval, the BIS is authorized to cooperate with more than a hundred of intelligence services. The BIS exchanges information and stays in contact mainly with services from EU and NATO countries. In terms of multilateral cooperation, the BIS participated in the work of all organizations of which it is a member (e.g. Counter-Terrorism Group or NATO Civilian Intelligence Committee).

The main areas of cooperation have been for some time the fight against terrorism, espionage, proliferation as well as cyber-security or protection of classified information and security eligibility screening. In 2022, the BIS

received more than 15 thousand documents from its partners and shared over two thousand documents. Representatives of the Service took part in over a thousand of international meetings on strategic and expert level. This year's increase in international meetings was the result of several factors.

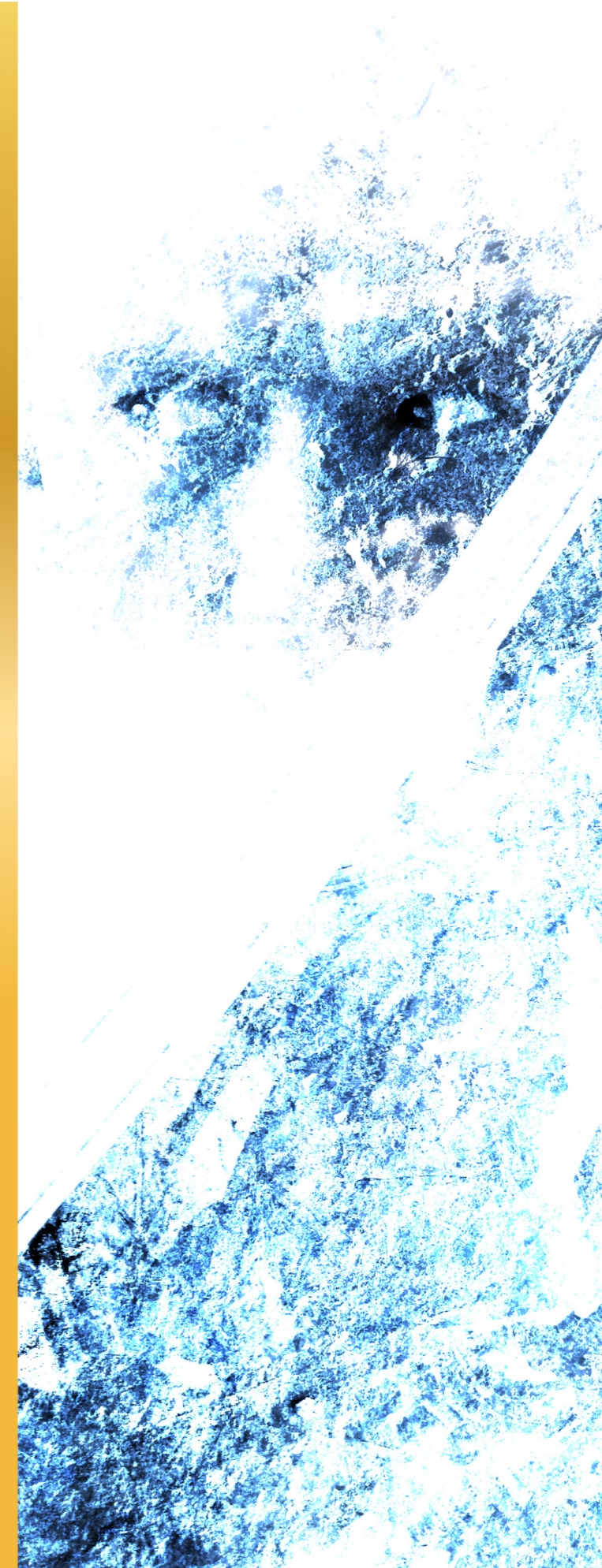
Since the beginning of the year, health protection measures linked to the COVID-19 pandemic were being gradually cancelled in most countries which are the BIS's partners, leading to gradual return to the same level of intensity in cooperation as prior to the pandemic. As a consequence of the Russian invasion of Ukraine, there was also an increase in information exchange and cooperation due to the need to coordinate the response to new threats emanating from the Russian aggression and unstable situation in Ukraine.

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 the 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 information and documents specified by the law to the Oversight Commission.



Internal Oversight and Internal Audit

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, assume 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 operations 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 requests 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 the security situation are available.

Expert units of the BIS conducted 37 inspections. Their aim was to methodically and factually guide the operation of organizational units in the financial and material area, enforce the 3E principle 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 major infringement of regulations was uncovered during these inspections.

The BIS sickness insurance body carried out 13 inspections of persons temporarily unable to work as defined by Section 76 of Act No. 187/2006 Coll. No infringements of regulations were uncovered.

Employees of the archive and of the control group carried out 62 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 etc., as amended. In 2022, three audits were completed. No severe infringement that could adversely influence activities of the Service or signalize reduced quality of its internal oversight system were identified.

External Oversight

In 2022, the health department of the Ministry of the Interior conducted three inspections in the catering facilities of the BIS, focusing on nutritional norms stipulated by Act No. 258/2000 Coll. on the Protection of Public Health, Government Decree No. 361/2007 Coll. and other relevant legislation. The inspections identified no infringement of applicable norms and regulations.

Service Discipline, 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 misdemeanor and of a disciplinary infractions by a BIS officer, 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.

The majority of investigations of conduct suspected of having the traits of misdemeanor 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 misdemeanor by a

BIS member were referred to a disciplinary proceeding.

One of 110 reports was evaluated as a complaint about the conduct of a BIS officer. The complaint was found groundless. 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 Czechia and abroad, and situation concerning the war in Ukraine.

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

The Inspection Department assumes the role of the Police in criminal proceedings and its work is supervised by the public prosecutor office which has jurisdiction *ratione materiae* or *ratione loci* depending on the case in question.

Budget

In 2022, the budget of the BIS was stipulated by the Act No. 57/2022 Coll., on the State Budget of the Czech Republic for 2022. Approved revenues amounted to CZK 2.5 billion and expenditures CZK 2 120 190 000.

Besides, the BIS registered claims to unconsumed expenditures. Total budget of expenditures, i.e. all available resources including applied claims to unconsumed expenditures, amounted to CZK 2 734 995 000 as of 31 December 2022.

Service's funds were mainly invested in maintaining the serviceability of the material and technical base and its necessary development. The most important project continued to be the construction of a technical and administrative compound. Further expenditures were made in order to ensure necessary maintenance and essential improvements of the Service's current assets.

An important investments were made to modernize surveillance equipment as well as information and communications systems. Last but not least, further renewal of the vehicle fleet took place.

Payroll expenses again accounted for the majority of regular expenditures, consisting mainly of salaries and related payments. The expenditures regarding pensions to which former long-term servicemen are entitled continue to grow steadily.

Further regular expenditures were comprised mainly of spending on special

equipment and special funds necessary for intelligence activities.

Other service and maintenance expenditures included common material expenditures, expenditures for the purchase of services and energies necessary for daily operations of the Service, and outsourced services and maintenance of property and compounds of the Service. The volume of service and maintenance expenditures in 2022 was to some extent influenced by the growing prices of a number of commodities and services which are essential for the functioning of the Service and the fulfillment of its tasks. Despite these negative external factors, essential needs of the Service were successfully addressed.

The budget allowed the Service to cover its basic service and maintenance expenditures in 2022. Given the limited amount of funds, the Service was required to use remaining claims to unconsumed expenditures to finance the final stages of the construction of the new technical and administrative compound. It was only thanks to the unconsumed expenditure claims that the construction could continue.

A detailed report on the Service's budgetary management in 2022 as required by the applicable decree of the Ministry of Finance was submitted to the Ministry and to the Security Committee of the Chamber of Deputies of the Parliament of the Czech Republic.

**Annual Report
of the Security Information Service
for 2022**

Bezpečnostní informační služba
P. O. BOX 31
155 00 Prague 515
Czech Republic
Phone: +420 235 521 400
Fax: +420 235 521 715
E-mail: info@bis.cz
Data box: cx2aize

